



CTPATTM

YOUR SUPPLY CHAIN'S STRONGEST LINK.

MSC Education, Training, and Awareness



U.S. Customs and
Border Protection

12.1 CORE (ALL)

- Members **MUST** establish and maintain a security awareness and training program to recognize and promote/foster awareness of facility, transportation and cargo security vulnerabilities at each point in the supply chain, which could be exploited by terrorists or smugglers.



U.S. Customs and
Border Protection

12.1 CORE

- Members **MUST** establish and maintain a security awareness and training program to recognize and promote/foster awareness of facility, transportation and cargo security vulnerabilities at each point in the supply chain, which could be exploited by terrorists or smugglers.



Indonesia Suffers Its Worst Terrorist Attack in a Decade. Here's What to Know About the Latest Wave of Violence



Bomb attack on church in southern Philippines kills 20



12.1 CORE

- The training program **MUST be comprehensive and cover all CTPAT security requirements.**



12.1 CORE

Focus Areas	Criteria Categories	Description
Corporate Security	Security and Responsibility Vision (New)	Promote a security vision, integrate security across the organization, establish an audit process and the importance and role of CTPAT POC
	Risk Assessment	Complete a comprehensive risk assessment based on a recognized methodology in line with the MSC.
	Requirements for Business Partners	Select, Assess and Monitor Business Partner Compliance with MSC to Include Trade-Based Money Laundering
	Cybersecurity (New)	Written cybersecurity policies and procedures; computer system software and hardware protection; remote access; personal devices.
Transportation Security	Transportation Security and IIT	Conduct comprehensive inspections for both security and visible agricultural contamination; driver verification; transport tracking; random searches.
	Seal Security	High Security Seal Policy; containers not suitable for sealing; required use of the VVTT seal verification process; Seal management audits.
	Procedural security	Document relevant processes for cargo transportation, handling and storage. Verification and preparation of documentation, manifest, BOL, etc.
	Agricultural Security (New)	Introduces requirements that protect supply chain from contaminants and pests and the proper use of wood packaging materials.
Personnel and Physical Security	Physical Access Controls	Describes requirements to prevent, detect, or deter unauthorized personnel from accessing the facilities. Expands on the use of security technology.
	Physical security	Require positive identification of all employees, visitors, and vendors at all points of entry.
	Personnel Security	Complete the assessment, pre-employment check, background check, and comply with U.S. immigration laws.
	Security Training, Threat Awareness	Requires security training for all employees; specialized training for employees in sensitive positions; determine if the training provided was effective (tests-drills)



12.1 CORE

- Staff at **sensitive positions** **MUST** receive additionally **training specialized** to the responsibilities of the position.



12.1 CORE

- **One of the key aspects of a security program is training.** Employees who understand why security measures exist are more likely to follow them. Safety training **MUST** be provided to employees on a regular basis, as required by their roles and titles, and newly hired employees **MUST** receive this training as part of their work orientation or initiation.



- Members **MUST** maintain evidence of training, such as training records, log sheets (roster), or electronic training records.
- Training records **MUST** include the training date, the names of those who attended, and training topics.



2020

[illegible]

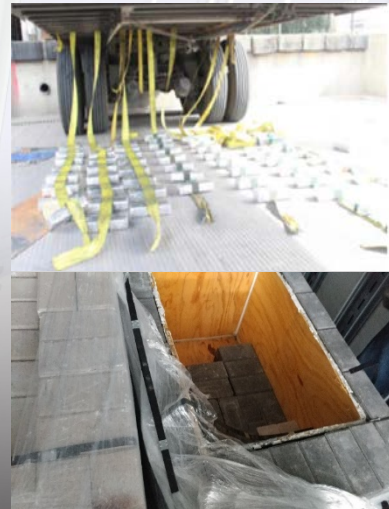
12.1 Implementation Guidance

- Training topics may include protecting access controls, recognizing internal conspiracies, and reporting procedures for suspicious activities and security incidents. Whenever possible, specialized training should include a practical demonstration. If there is a practical demonstration, the instructor should give students time to demonstrate the process.
- For CTPAT purposes, positions of trust include personnel who work directly with import and export cargo or its documentation, as well as personnel involved in controlling access to sensitive areas or equipment. Said positions include, but are not limited to, shipping, receiving and correspondence personnel, drivers, dispatchers, security guards, and anyone involved in cargo assignments, monitoring of modes of transportation, and seal control.



12.2 IMP/EXP/FM/CON/BRO/HC/AIR/3PL/RAIL

- Drivers and other personnel conducting agricultural and security inspections of empty conveyances and instruments of international traffic (IITs) **MUST** be trained to inspect their transports/IITs for both agricultural and security purposes.
- Refresher training **MUST** take place periodically, as needed after an incident or security breach, or when there are changes to company procedures.
- "Inspection training **MUST** include the following topics:
 - Signs of hidden compartments;
 - Illegal smuggling hidden in natural compartments; and
 - Signs of contamination by pests. "



12.3 HC/LH/RAIL/3PL

- Staff **MUST** receive training on situational reporting: procedures to follow if something is found during a transportation inspection or if a safety incident occurs during transit.
- **Report Policy-undercarriage**
- **Contact CBP**
 - **Port of Entry**
 - **SCSS**

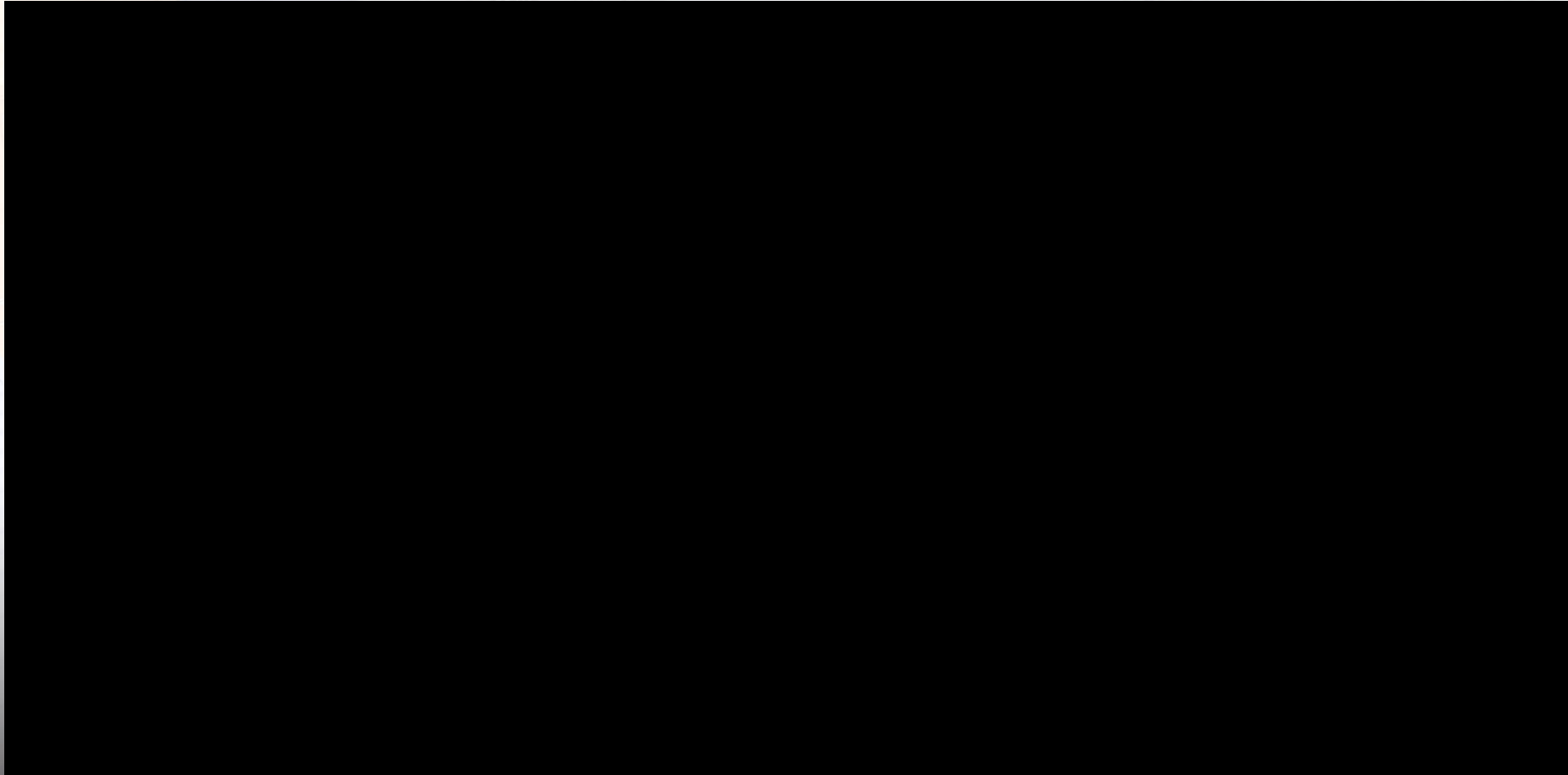


12.3 HC/LH/RAIL/3PL

- In addition, personnel **MUST** be instructed to check/use seals during transit, and to look for signs of someone observing the movement of transport and/or goods.
- Understand seal policies
- How to place seals
- Second Seal Policy



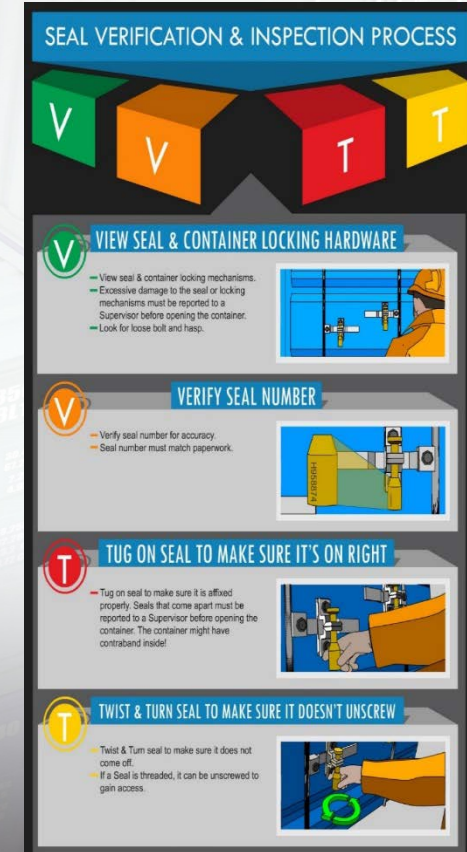
12.3 HC/LH/RAIL/3PL



12.3 HC/LH/RAIL/3PL

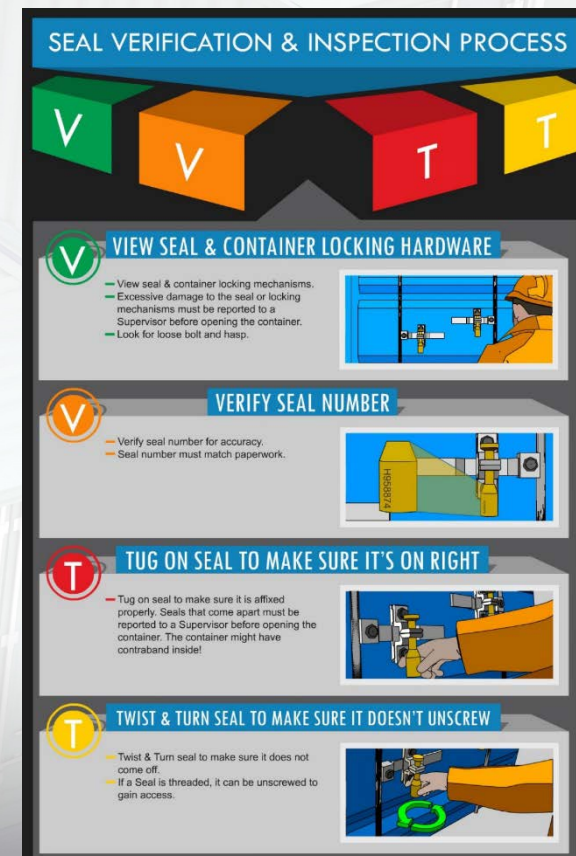
continued....

- Drivers **MUST** receive training on how to conduct the Seal Verification Process (VVTT).
- The verification process for the CTPAT seal is as follows:
 - V - View closing mechanisms of the seal and the container
 - V - Verify seal number against the shipping documents
 - T - Tug seal to make sure it is positioned correctly
 - T - Twist and turn the bolt seal to make sure its components will not unscrew or separate from each other.



12.3 HC/LH/RAIL/3PL

continued....



12.4 CORE

- CTPAT members **MUST** have measures in place to verify that the training provided meets all the training objectives.

Electronic Training,
Testing, Games, etc.



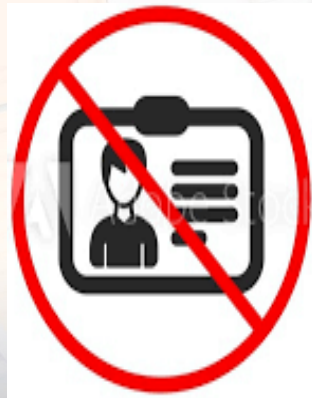
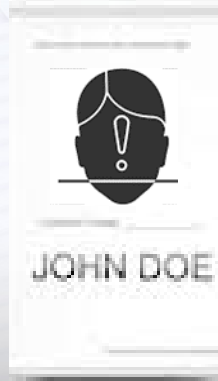
12.4 Implementation Guidance

Understanding the training and being able to use that training in one's position (for sensitive employees) is of the utmost importance. **Exams or quizzes...**



12.4 Implementation Guidance

... A(n) **exercise/drill**, or periodic audits of procedures, etc., are some of the measures that the Member can implement to determine effectiveness of the company's policies, training and general security program.

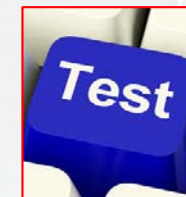


Conduct mini-audits:
collect all the documents
involved in CTPAT for its
effectiveness.



12.4 Implementation Guidance

... A(n) **exercise/drill**, or periodic audits of procedures, etc., are some of the measures that the Member can implement to determine effectiveness of the company's policies, training and general security program.



12.5 Brokers

- Customs Brokers **MUST** be able to explain CTPAT's security requirements to their importer clients, apprise them of critical program developments, and encourage those importers to become CTPAT Members.



12.5 Implementation Guidance

The broker may create opportunities to educate the importing community on CTPAT policy and on topics where the broker has relevant expertise, which might include security procedures, best practices, access controls, documentation fraud, information security, internal conspiracies, and technologies that further the goal of a secure global supply chain. These interactions may focus on employees working in sensitive positions such as shipping, information technology, receiving, and mailroom processing.

12.6 IMP/EXP/BRO

- Specialized training **MUST** be given annually to staff who can identify warning indicators of trade-based money laundering and terrorist financing.



12.6 Implementation Guide

Personnel who will receive such training include those responsible for business compliance, sales, security, procurement, finance, shipping, and receiving shipments. Members can take into account the document of the **CTPAT Warning Indicators for Trade-Based Money Laundering and Terrorism Financing Activities.**

12.7 HC/LH/3PL/IMP/EXP/SEA/AIR/RAIL

- Training **MUST** be provided to appropriate personnel to prevent visible pest contamination.
- The training **MUST** cover pest prevention measures, regulatory requirements for wood packaging materials (WPM), and identification of infested wood.







12.7 Implementation Guidance

Public Library

C-TPAT Partner Library

Search

View	Name	Type	Size	Uploaded By	Uploaded Date
	Southern Border Truck Contaminants_Trade Outreach_May 2018.pptx	Training	7.1 MB	Carlos Ochoa	07/24/2018 15:10
	Seaport Pest Contaminants_Trade Outreach_May 2018.pptx	Training	7.5 MB	Carlos Ochoa	07/24/2018 15:08
	Northern Border Truck Contaminants_Trade Outreach_May 2018.pptx	Training	7 MB	Carlos Ochoa	07/24/2018 15:07
	Rail Pest Contaminants_Trade Outreach_May 2018.pptx	Training	13 MB	Carlos Ochoa	07/24/2018 15:07



12.8 CORE

- As appropriate in their roles and/or positions, staff **MUST** receive training on the company's cybersecurity policies and procedures.
- This **MUST** include the need for employees to protect passwords/passphrases and computer access.



12.8 Implementation Guidance

Training quality is important for decreasing vulnerability to cyberattacks. A robust cybersecurity training program is typically delivered to appropriate staff in a formal setting rather than simply through emails or notes.

Password: flaviogarza1234 ❌

Password: fguoFH\$9821 ✅



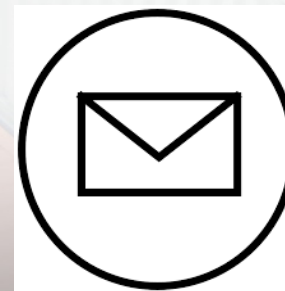
12.9 CORE

- Personnel who operate and manage security technology systems **MUST** have received training in their operation and maintenance.
- Previous experience with similar systems is acceptable. Self-training through operating manuals and other methods is acceptable.
- <https://www.infragard.org> It is a partnership between the FBI and members of the private sector.



12.10 CORE


- Staff **MUST** receive training on how to report security incidents and suspicious activities.



12.10 CORE

If you see something, say something

What is Sus



Accept the challenge

Do you pay attention to your surroundings?

Watch the videos to find out. Then share the videos with your friends to see how they do.


Bikes

Take Action


Together, we can help keep our communities safe.

DHS created these videos to raise awareness of the importance of paying attention to your surroundings.

- Share this page with your friends on [Facebook](#) and [Twitter](#)!
- Learn how you can [help protect your community](#)
- Represent a University? [Help spread the word!](#)



About the Campaign





12.10 Implementation Guidance

Procedures for reporting security incidents or suspicious activities are extremely important aspects of a security program, and training on how to report an incident can be included in general security training. Specialized training modules (based on job tasks) can have more detailed training on reporting procedures, to include details about the process: what to report, to whom, how to report it, and what to do next after reporting.

**SUSPECT IT ?
REPORT IT**



U.S. Customs and
Border Protection



Reporting to U.S. Customs and Border Protection (CBP)

Laredo POE:

Phone #	956-794-9419
Phone #	956-417-5151
Fax #	956-794-9448/956-417-5131
Email	ATULAREDO@cbp.dhs.gov

C-TPAT assigned SCSS:

Phone #	281-594-5427
Cell #	281-687-2206
e-mail	Flavio.garza@dhs.gov

National Hotline Reporting Suspicious Activity:

1-800-Be-Alert

*Please ensure to contact the appropriate CBP office and/or appropriate foreign authority:

- 1) Any time there are compromised high security seals detected.
- 2) Anytime there is container/trailer integrity issues detected (found concealment compartments, door hardware tampering, or container/ trailer structural anomalies).
- 3) Anytime you suspect or detect any anomalies, suspicious, and/or illegal activities related to security issues.
- 4) If any contamination of trailers/containers and cargo is detected.



U.S. Customs and
Border Protection

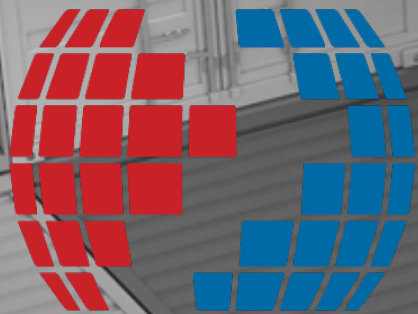


YOUR SUPPLY CHAIN'S STRONGEST LINK.

CBP Publication Number 0413-0211
March 2011

Questions





CTPATTM

YOUR SUPPLY CHAIN'S STRONGEST LINK.



U.S. Customs and
Border Protection