
CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.
Physical Access Control
U.S. Customs and
Border Protection

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

10.1 CORE

- CTPAT members MUST have written procedures regulating how ID badges and access devices are issued, changed, and withdrawn.
- Where applicable, a personnel identification system MUST be in place for positive identification and access control purposes.
- Access to sensitive areas MUST be restricted based on job description or assigned tasks.
- Withdrawal of access devices MUST take place once the employee leaves the company.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

10.1 Implementation Guide

- Physical access devices include identification badges, temporary visitor and vendor badges, biometric identification systems, proximity cards, codes, and keys. When employees are separated from a company, the use of termination logs helps ensure that all access devices have been returned and/or disabled. In general, an identification system is required for companies with more than 50 employees.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

10.2 CORE

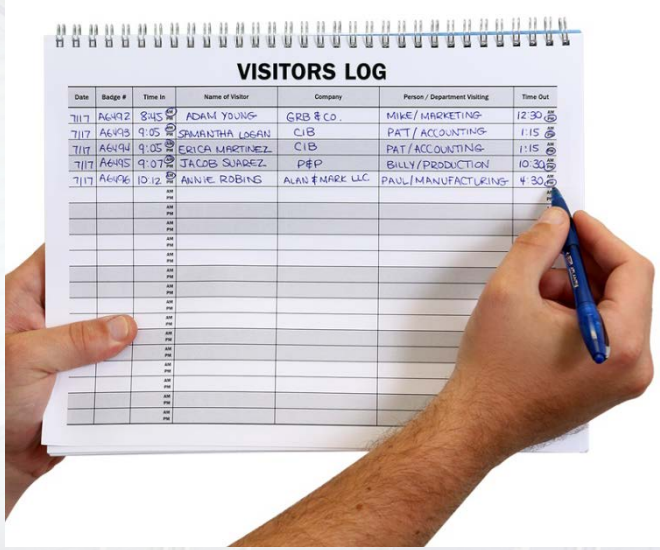
- In general, for companies with 50 or more employees, staff MUST use a company-issued identification credential that must be displayed at all times when on the premises (except when this creates a hazard).
- All visitors, vendors, and service providers MUST present photo identification upon arrival. A record MUST be kept to document the details of the visit.
- In addition, all visitors and service providers MUST receive a temporary ID. If temporary identification is used, it MUST be visibly displayed at all times during the visit.
- All visitors MUST be escorted at all times.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

10.2 CORE

The record must include the following:

- Date of the visit;
- Visitor's name;
- Photo ID verification (verified type, such as a national ID card or license).
- Arrival time;
- Company Point of Contact; and
- Departure time.



Frequent and well-known visitors, such as regular vendors, may be exempted from verification but still need to be registered upon entering/exiting the premises.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

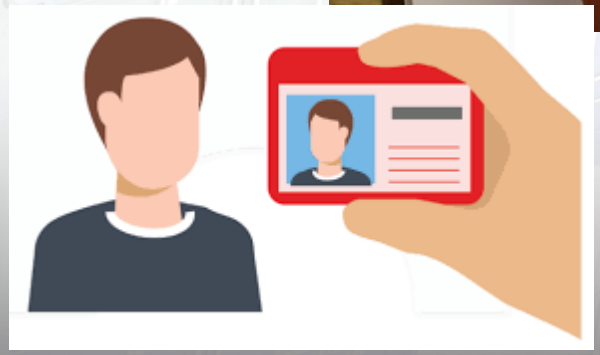
10.3 IMP/EXP/FM/CON/HC/LH/MPTO/3PL/BRO

- Drivers delivering or receiving cargo MUST be positively identified before receiving or releasing cargo.
- Drivers MUST present a government-issued photo ID to the facility employee granting access to verify their identity. If it is not feasible to present a government-issued photo ID, the facility employee may accept a photo ID issued by the carrier employing the driver picking up the load.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

10.4 IMP/EXP/FM/CON

- A log MUST be kept to record drivers picking up cargo and the details of their transportation units.
- When drivers arrive to pick up cargo at a facility, a facility employee MUST record them in the log.
- Driver departure MUST also be recorded in the log.
- This log MUST be kept secure and drivers MUST NOT have access to it.



CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

10.4 CORE

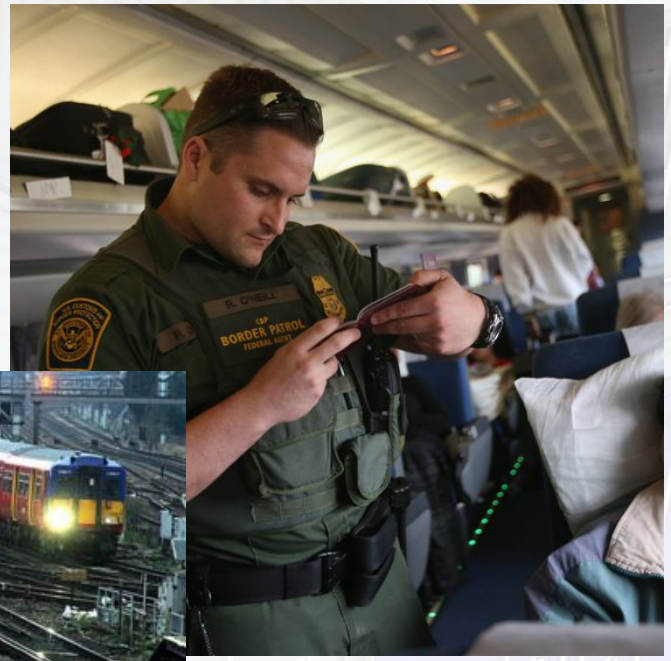
The log used to document driver arrival/departure must contain the following elements:

- Driver name;
- Arrival date and time;
- Employer;
- Truck number;
- Trailer number;
- Departure date and time;
- Seal number affixed to the trailer at time of departure.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

10.5 RAIL

- Per CBP requirements, all train personnel MUST be identified.



CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

10.6 RAIL

- Rail carriers MUST focus their community security and intrusion reduction programs on areas adjacent to company-designated critical infrastructure.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

10.7 HC/FM/IMP/EXP/3PL

- Before arriving at the customer's premises, the carrier MUST notify of approximate arrival time for the scheduled pickup, the driver's name, and the truck number.
- When operationally feasible, CTPAT members MUST allow shipments and deliveries by appointment only.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

10.8 CORE

- Packages and mail MUST be periodically scanned for contraband before being admitted.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

10.9 CORE

- Delivery of goods to the consignee, or other persons who accept cargo delivery at the partner's premises, MUST be limited to a specific and monitored area.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

10.10 IMP/EXP/CON/FM/3PL/RAIL/HC/AIR/MPTO/SEA/LH

- If security guards are used, work instructions for guards MUST be contained in written policies and procedures.
- Management MUST periodically verify compliance and adequacy of these procedures through audits and policy reviews.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

10.11 MPTO

- Marine Port Terminal Operators (MPTO) security personnel MUST meet regularly with government police assigned to the port and vessel security personnel.
- If a Facility Security Officer (FSO) has been designated per the Maritime Transportation Security Act of 2002 (MTSA) and / or the International Ship and Port Facility Security (ISPS) Code, the FSO SHOULD be the MPTO's point-of-contact for all CTPAT's matters relating to security
- MPTOs operating in an international port with a Container Security Initiative (CSI) contingent SHOULD make every effort to maintain regular liaison with the Team Leader of the CSI contingent, as a forum to discuss supply chain security issues and to gauge and evaluate current approaches to security and targeting.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

10.11 Implementation Guide

- "The International Maritime Organization's ISPS Code is a comprehensive set of measures to enhance the security of ships and port facilities. Having come into force in 2004, it prescribes responsibilities to governments, shipping companies, shipboard personnel, and port/facility personnel to detect security threats and take preventative measures against security incidents affecting ships or port facilities used in international trade. MTSA is a US law designed to increase the security of our Nation's seaports. Among other things, it requires vessels and port facilities to conduct vulnerability assessments and develop security plans. This law is the US implementation of the ISPS Code. "


CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.
U.S. Customs and
Border Protection