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

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.1 CORE

- All cargo handling and storage facilities, including trailer yards and offices, MUST have physical barriers and/or deterrents that prevent unauthorized access.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.2 CORE

- Perimeter fencing MUST enclose areas around cargo handling and storage facilities.
- If a facility handles cargo, interior fencing MUST be used to secure cargo and cargo handling areas.
- Depending on the hazard, the additional interior fencing MUST segregate various types of cargo, such as domestic, international, high-value, and/or hazardous materials.
- Fences MUST be periodically inspected for integrity and damage.
- If fence damage is found, repairs MUST be done as soon as possible.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.4 CORE

- Doors where vehicles and/or personnel enter or exit (as well as other exit points) MUST be manned or monitored. People and vehicles may be subject to search in accordance with local and labor laws.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.5 CORE

- Private vehicles MUST be prohibited from parking in adjacent cargo handling and storage areas and means of transportation.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

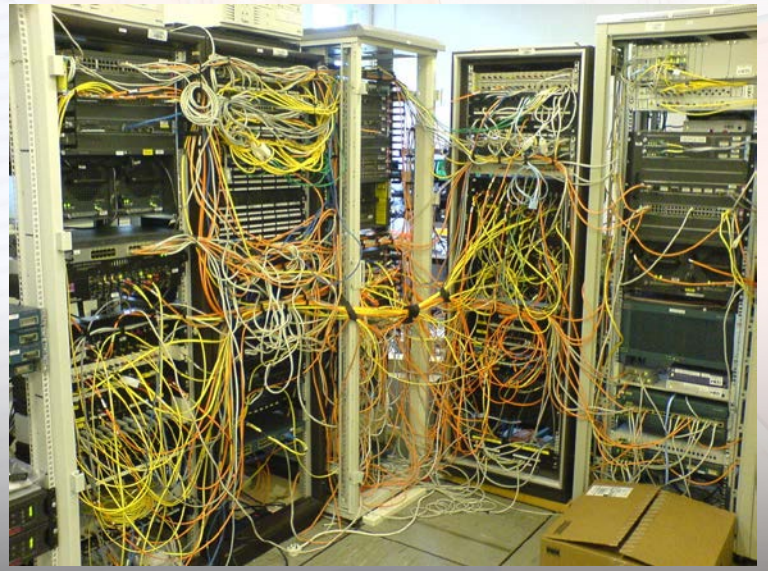
9.6 CORE

- Adequate lighting MUST be provided inside and outside the facility, including, as appropriate, the following areas: entrances and exits, cargo handling and storage areas, perimeter fence, and parking areas.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.7 CORE

- Security technology MUST be used to monitor facilities and prevent unauthorized access to sensitive areas.



CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.8 CORE

- Members who rely on technology security for physical security MUST have written policies and procedures that govern the use, maintenance, and protection of this technology.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.8 CORE

- At a minimum, these policies and procedures MUST provide:
  - The way in which access to places where technology is controlled/managed or where its hardware is maintained (control panels, video recording units, etc.) is limited to authorized personnel;
  - Procedures that have been implemented to test/inspect the technology on a regular basis;
  - Inspections that include verifications of the correct equipment operation and, if applicable, equipment that is positioned correctly;
  - Documented results of inspections and performance tests;
  - If corrective actions are necessary, they must be implemented as soon as possible and corrective actions taken are documented;
  - Inspection results are documented long enough for auditing purposes.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.8 CORE

- If a third-party (external) central monitoring station is used, the CTPAT member MUST have written procedures stipulating the functionality of critical systems and authentication protocols including (but not limited to) changes to the security code, adding or by subtracting authorized personnel, password checks, and system access or denial.
- Security technology policies and procedures MUST be reviewed and updated annually, or more frequently, as risk or circumstances dictate.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.9 CORE

- CTPAT members MUST utilize licensed/certified resources when considering security technology design and installation.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

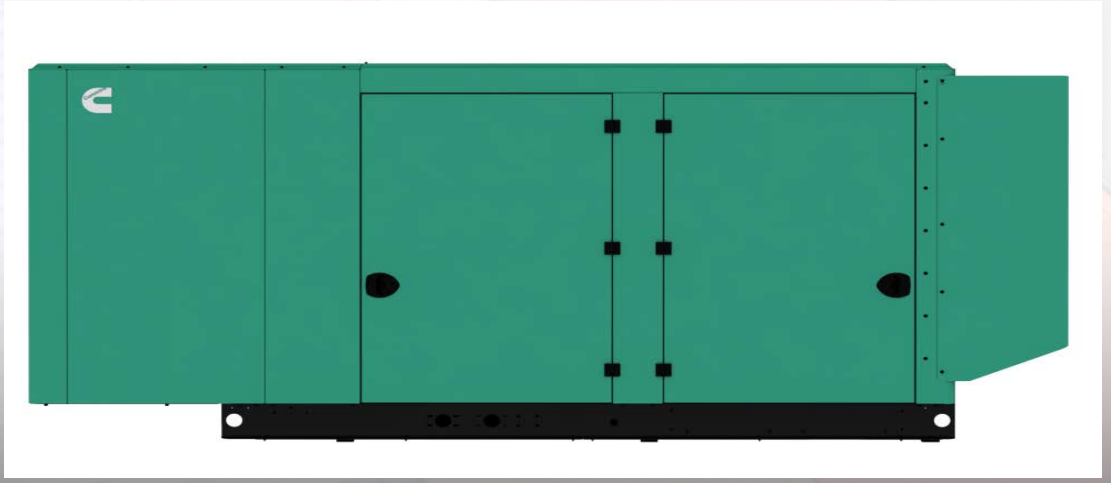
9.10 CORE

- All security technology infrastructure MUST be physically protected from unauthorized access.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.11 CORE

- Safety technology systems MUST be configured with an alternative power source that allows systems to continue to operate in the event of an unexpected loss of direct power.



CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.12 CORE

- If camera systems are implemented, cameras MUST monitor the premises and sensitive areas of the premises to prevent unauthorized access.
- Alarms MUST be used to alert businesses of unauthorized access to sensitive areas.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.13 CORE

- If camera systems are implemented, cameras MUST be positioned to cover key areas of the facility pertaining to import/export processes.
- The cameras MUST be programmed to record at the highest image quality setting reasonably available, and configured to record 24 hours a day, 7 days a week.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.14 CORE

- If camera systems are implemented, cameras MUST have a function that indicates/reports an "operation/recording failure" condition.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.15 CORE

- If camera systems are implemented, periodic and random reviews of the recordings MUST be conducted (by management, security or other designated personnel) to verify that cargo security procedures are properly followed in accordance with the law.
- Results of the reviews MUST be summarized in writing and include any corrective actions taken.
- Results MUST be maintained long enough for audit purposes.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.15 Implementation Guide

If camera footage is only reviewed for cause (as part of an investigation following a security breach, etc.), you don't get the full benefit of having cameras. They are not just investigation tools; used proactively, they can help prevent a security breach.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

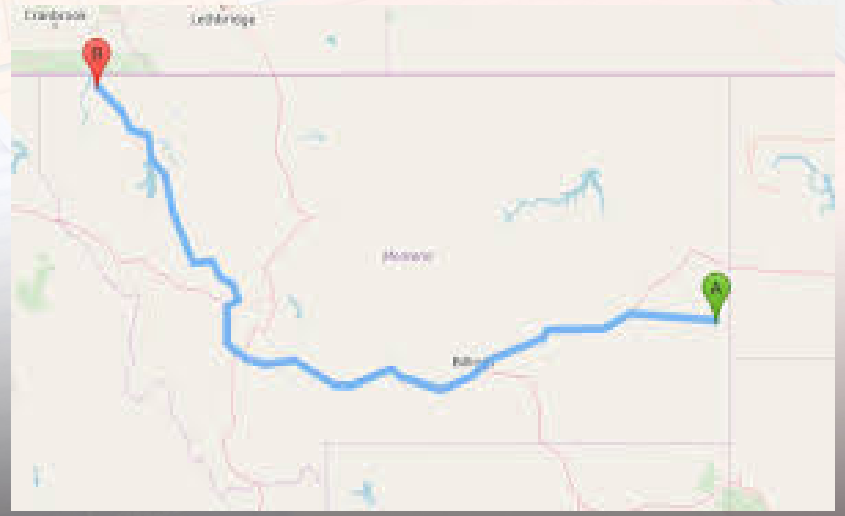
9.15 Implementation Guide

- Focus random reviews of recordings on the physical chain of custody to ensure that the shipment remains secure and all security protocols are followed. Some examples of processes that can be reviewed are as follows:
  - Cargo handling activities;
  - Container inspections;
  - The loading process;
  - The sealing process;
  - Unit arrival/departure; and
  - Load departure, etc.
- Purpose of the review:
  - The purpose is to evaluate the overall adherence and effectiveness of established security processes, identify vulnerabilities or weaknesses, and order corrective actions to support improving security processes. Member can perform a periodic review according to risk (previous incidents or an anonymous report about an employee not following safety protocols on the platform, etc.).
- Items to include in the written summary:
  - Review date;
  - Date of the footage that was reviewed;
  - What camera/area the recording was from;
  - Brief description of any findings; and
  - If corrective actions are warranted.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

9.16 CORE

- If cameras are used, recordings covering key import/export processes MUST be kept long enough for an investigation of a monitored shipment to be accomplished.



CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

Questions/Discussion


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