

Importers: C-TPAT Minimum Security Requirements

**Customs and Border Protection, U.S. Department of Homeland Security
C-TPAT Minimum Security Requirements
Importers
Released March, 2005**

Importers: C-TPAT Minimum Security Requirements

Suggested Compliance Responses

Suggested status responses to “general statements” are: Strongly Disagree, Disagree, Agree, Strongly Agree, and N/A.

Suggested status responses to “specific criteria/requirements” are: Not Compliant, Partially Compliant, Compliant, Exceeds Requirement, and N/A.

Importers: C-TPAT Minimum Security Requirements

Minimum Security Requirements: Importers

1.0.0 C-TPAT Security Criteria Overview

1.1.0 Definitions

1.1.1 The supply chain for C-TPAT purposes is defined from point of origin (manufacturer, supplier, or vendor) through to point of distribution; it recognizes the diverse business models C-TPAT members employ.

1.2.0 C-TPAT Acknowledgements

1.2.1 The C-TPAT program recognizes the complexity of international supply chains and security practices, and endorses the application and implementation of security measures based upon risk.

1.2.2 The C-TPAT program allows for flexibility and the customization of security plans based on the member's business model.

1.3.0 Basic Requirements

1.3.1 Importers must conduct a comprehensive assessment of their international supply chains based upon C-TPAT security criteria.

1.3.2 Where an Importer outsources or contracts elements of their supply chain, such as a foreign facility, conveyance, domestic warehouse, or other elements, the Importer must work with these Business Partners to ensure that pertinent security measures are in place and adhered to throughout their supply chain.

1.3.3 Appropriate security measures, based upon risk, must be implemented and maintained throughout the Importer's supply chains.

Importers: C-TPAT Minimum Security Requirements

2.0.0 Business Partner Requirement

2.1.0 Business Partner Security Requirements: General statement

2.1.1 Importers must have written and verifiable processes for the selection of Business Partners including manufacturers, product suppliers and vendors.

2.2.0 Business Partner Security Procedures

2.2.1 For those Business Partners eligible for C-TPAT certification (carriers, ports, terminals, brokers, consolidators, etc.) the Importer must have documentation (e.g., C-TPAT certificate, SVI number, etc.) indicating whether these Business Partners are or are not C-TPAT certified.

2.2.2 For those Business Partners not eligible for C-TPAT certification, Importers must require their Business Partners to demonstrate that they are meeting C-TPAT security criteria via either: written/electronic confirmation (e.g., contractual obligations; via a letter from a senior Business Partner/Officer attesting to compliance; a written statement from the Business Partner demonstrating their compliance with C-TPAT security criteria or an equivalent WCO accredited security program administered by a foreign customs authority; or, by providing a completed Importer security questionnaire).

2.2.3 Based upon a documented risk assessment process, non-C-TPAT eligible Business Partners must be subject to verification of compliance with C-TPAT security criteria by the Importer.

Status	Comment - General
Status	Comment - Specific

Importers: C-TPAT Minimum Security Requirements

2.3.0 Point of Origin

2.3.1 Importers must ensure Business Partners develop security processes and procedures consistent with the C-TPAT security criteria to enhance the integrity of the shipment at point of origin.

2.3.2 Periodic reviews of Business Partners' processes and facilities should be conducted based on risk, and should maintain the security standards required by the Importer.

2.4.0 Participation and/or Certification in Foreign Customs Administrations Supply Chain Security Programs

2.4.1 Current or prospective Business Partners who have obtained a certification in a supply chain security program being administered by foreign Customs Administrations should be required to indicate their status of participation to the Importer.

2.5.0 Other Internal Criteria for Business Partner Selection

2.5.1 Internal requirements, such as financial soundness, capability of meeting contractual security requirements, and the ability to identify and correct security deficiencies as needed, should be addressed by the Importer.

2.5.2 Internal requirements should be assessed against a risk-based process as determined by an internal management team.

Status	Comment - Specific
Status	Comment - Specific
Status	Comment - Specific

Importers: C-TPAT Minimum Security Requirements

3.0.0 Container Security

3.1.0 Container Security Requirement

- 3.1.1 Container integrity must be maintained to protect against the introduction of unauthorized material and/or persons.
- 3.1.2 At point of stuffing, procedures must be in place to properly seal and maintain the integrity of the shipping containers.
- 3.1.3 A high security seal must be affixed to all loaded containers bound for the U.S.
- 3.1.4 All seals must meet or exceed the current PAS ISO 17712 standards for high security seals.

Status	Comment - Specific

Importers: C-TPAT Minimum Security Requirements

4.0.0 Container Inspection

4.1.0 Container Inspection Requirements: General Statement

4.1.1 Procedures must be in place to verify the physical integrity of the container structure prior to stuffing, to include the reliability of the locking mechanisms of the doors.

4.2.0 Container Inspection Requirements

4.2.2 A seven-point inspection process is recommended for all containers: front wall; left side; right side; floor; ceiling/roof; inside/outside doors; and, outside/undercarriage.

4.3.0 Container Seals

4.3.1 Written procedures must stipulate how seals are to be controlled and affixed to loaded containers.

4.3.2 The procedures will include procedures for recognizing and reporting compromised seals and/or containers to US Customs and Border Protection, or the appropriate foreign authority.

4.3.3 Only designated employees should distribute container seals for integrity purposes.

4.4.0 Container Storage

4.4.1 Containers must be stored in a secure area to prevent unauthorized access and/or manipulation.

4.4.2 Procedures must be in place for reporting and neutralizing unauthorized entry into containers or container storage areas.

Status	Comment - General
Status	Comment - Specific
Status	Comment - Specific
Status	Comment - Specific

Importers: C-TPAT Minimum Security Requirements

5.0.0 Physical Access Controls

5.1.0 Physical Access Security Requirements: General Statement

5.1.1 Access controls prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, and vendors at all points of entry.

5.2.0 Employees

5.2.1 An employee identification system must be in place for positive identification and access control purposes.

5.2.2 Employees should only be given access to those secure areas needed for the performance of their duties.

5.2.3 Company management or security personnel must adequately control the issuance and removal of employee, visitor and vendor identification badges.

5.2.4 Procedures for the issuance, removal and changing of access devices (e.g. keys, key cards, etc.) must be documented.

5.3.0 Visitors

5.3.1 Visitors must present photo identification for documentation purposes upon arrival.

5.3.2 Visitors should be escorted and visibly display temporary identification.

Status	Comment - Specific
Status	Comment - Specific
Status	Comment - Specific

Importers: C-TPAT Minimum Security Requirements

5.4.0 Deliveries (including mail)

5.4.1 Proper vendor ID and/or photo identification must be presented for documentation purposes upon arrival by all vendors.

5.4.2 Arriving packages and mail should be periodically screened before being disseminated.

5.5.0 Challenging and Removing Unauthorized Persons

5.5.1 Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.

Status	Comment - Specific
Status	Comment - Specific

Importers: C-TPAT Minimum Security Requirements

6.0.0 Personnel Security

6.1.0 Personnel Security Requirements: General Statement

6.1.1 Processes must be in place to screen prospective employees and to periodically check current employees.

6.2.0 Pre-Employment Verification

6.2.1 Application information, such as employment history and references, must be verified prior to employment.

6.3.0 Background Checks and Investigations

6.3.1 Consistent with foreign, federal, state, and local regulations, background checks and investigations should be conducted for prospective employees.

6.3.2 Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.

6.4.0 Personnel Termination Procedures

6.4.1 Companies must have procedures in place to remove identification, facility, and system access for terminated employees.

Status	Comment - General
Status	Comment - Specific
Status	Comment - Specific
Status	Comment - Specific

Importers: C-TPAT Minimum Security Requirements

7.0.0 Procedural Security

7.1.0 Procedural Security Requirements: General Statement

7.1.1 Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain.

7.2.0 Documentation Processing

7.2.1 Procedures must be in place to ensure that all information used in the clearing of merchandise/cargo, is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous information.

7.2.2 Documentation control must include safeguarding computer access and information.

7.3.0 Manifesting Procedures

7.3.1 To help ensure the integrity of cargo received from abroad, procedures must be in place to ensure that information received from Business Partners is reported accurately and timely.

7.4.0 Shipping and Receiving

7.4.1 Arriving cargo should be reconciled against information on the cargo manifest.

7.4.2 Arriving cargo should be accurately described, and the weights, labels, marks and piece count indicated and verified.

7.4.3 Departing cargo should be verified against purchase or delivery orders.

7.4.4 Drivers delivering or receiving cargo must be positively identified before cargo is received or released.

Status	Comment - General
Status	Comment - Specific
Status	Comment - Specific
Status	Comment - Specific

Importers: C-TPAT Minimum Security Requirements

7.5.0 Cargo Discrepancies

7.5.1 All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately.

7.5.2 If appropriate, Customs and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected.

Status	Comment - Specific

Importers: C-TPAT Minimum Security Requirements

8.0.0 Security Training and Threat Awareness

8.1.0 Threat Awareness

8.1.1 A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by drug smugglers and terrorists at each point in the supply chain.

8.1.2 Employees must be made aware of the procedures the Highway Carrier has in place to address a situation and how to report it.

8.1.3 Additional training should be provided to employees in the shipping and receiving areas, as well as those receiving and opening mail.

8.2.0 Security Training

8.2.1 Specific training should be offered to assist employees in maintaining cargo integrity, recognizing internal conspiracies, and protecting access controls.

8.3.0 Employee Incentives

8.3.1 Implemented programs should offer incentives for active employee participation.

Status	Comment - Specific
Status	Comment - Specific
Status	Comment - Specific

Importers: C-TPAT Minimum Security Requirements

9.0.0 Physical Security

9.1.0 Physical Security Requirements: General Statement

9.1.1 Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access. Importers should incorporate the following C-TPAT physical security criteria throughout their supply chains as applicable.

9.2.0 Fencing

9.2.1 Perimeter fencing should enclose the areas around cargo handling and storage facilities.

9.2.2 Interior fencing within a cargo handling structure should be used to segregate domestic, international, high value, and hazardous cargo.

9.2.3 All fencing must be regularly inspected for integrity and damage.

9.3.0 Gates and Gate Houses

9.3.1 Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored.

9.3.2 The number of gates should be kept to the minimum necessary for proper access and safety.

9.4.0 Parking

9.4.1 Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas.

9.5.0 Building Structure

9.5.1 Buildings must be constructed of materials that resist unlawful entry.

9.5.2 The integrity of structures must be maintained by periodic inspection and repair.

Status	Comment - General
Status	Comment - Specific
Status	Comment - Specific
Status	Comment - Specific
Status	Comment - Specific

Importers: C-TPAT Minimum Security Requirements

9.6.0 Locking Devices and Key Controls

9.6.1 All external and internal windows, gates and fences must be secured with locking devices.

9.6.2 Management or security personnel must control the issuance of all locks and keys.

9.7.0 Lighting

9.7.1 Adequate lighting must be provided inside and outside the facility at entrances and exits.

9.7.2 Adequate lighting must be provided inside and outside in cargo handling areas.

9.7.3 Adequate lighting must be provided inside and outside in storage areas.

9.7.4 Adequate lighting must be provided inside and outside along fence lines.

9.7.5 Adequate lighting must be provided inside and outside in parking areas.

9.8.0 Alarm Systems and Video Surveillance Cameras

9.8.1 Alarm systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas.

Status	Comment - Specific
Status	Comment - Specific
Status	Comment - Specific

Importers: C-TPAT Minimum Security Requirements

10.0.0 Information Technology Security

10.1.0 Password Protection

10.1.1 Automated systems must use individually assigned accounts that require a periodic change of password.

10.1.2 IT security policies, procedures and standards must be in place and provided to employees in the form of training.

10.2.0 Accountability

10.2.1 A system must be in place to identify the abuse of IT including improper access, tampering or the altering of business data.

10.2.2 All system violators must be subject to appropriate disciplinary actions for abuse.

Status	Comment - Specific
Status	Comment - Specific