Customs-Trade Partnership Against Terrorism (C-TPAT)

Exporter Eligibility Requirements

C-TPAT Exporter

Since its inception, the Customs-Trade Partnership Against Terrorism (C-TPAT) program has sought to enhance supply chain security throughout the international supply chain, from point of stuffing, through to the first U.S. port of arrival. As the C-TPAT program has continued its evolution, it has become apparent that exports also have an important role in international supply chains and while this sector is not as heavily owned by U.S. Customs and Border Protection (CBP) and the C-TPAT program, developing an export component for C-TPAT would further enhance both the program and its relationship with other mutually recognized Foreign Customs administrations.

Definition

For C-TPAT purposes, an exporter is defined as:

A person or company who, as the principal party in interest in the export transaction, has the power and responsibility for determining and controlling the sending of the items out of the United States.

Exporter Entity Eligibility Requirements

Entities that wish to participate in the C-TPAT Exporter program must meet with the program's definition of an Exporter as well as meet with the following eligibility requirements:

1. Be an active U.S. Exporter out of the United States.
2. Have a business office staffed in the U.S.
3. Be an active U.S. Exporter with a documentable

    a. Employee Identification Number (EIN),

    or

    b. Dun & Bradstreet (DUNS) number,

4. Have a documented export security program and a designated officer or manager who will act as the C-TPAT program main point of contact. Additionally the participant should have an alternate point of contact should the designated point of contact be unavailable.

5. Commit to maintaining the C-TPAT supply chain security criteria as outlined in the C- TPAT Exporter agreement.

6. Create and provide CBP with a C-TPAT supply chain security profile which identifies how the Exporter will meet, maintain, and enhance internal policy to meet the C-TPAT Exporter security criteria.

7. In order to be eligible the Exporter must have an acceptable level of compliance for export reporting for the latest 12-month period and be in good standing with U.S. Regulatory Bodies such as: Department of Commerce, Department of State, Department of Treasury, Nuclear Regulatory Commission, Drug Enforcement Administration, and Department of Defense.

Exporter Minimum Security Criteria

C-TPAT recognizes the complexity of international supply chains and endorses the application and implementation of security measures based upon risk analysis by exporters. Therefore, the program allows for flexibility and the customization of security plans based on the member's business model. Appropriate security measures, as listed throughout this document, must be implemented and maintained throughout the above C-TPAT export participants' supply chains. Exporters must conduct a comprehensive risk assessment of their international supply chain based upon the following C-TPAT security criteria. Where an exporter outsources or contracts elements of its supply chain, such as to a warehouse, logistics provider, carrier or other export supply chain element, the exporter must work with these business partners to ensure that effective security measures are in place and adhered to throughout the entire supply chain.

Business Partner Requirements

Exporters must have written and verifiable processes for the screening and selection of business partners including service providers, manufacturers, product suppliers, and vendors. Where applicable, these processes must include checks against the Department of Commerce/Bureau of Industry and Security (BIS), Department of State/Directorate of Defense Trade Controls (DDTC), and Department of Treasury/Office of Foreign Assets Control (OFAC) lists. Entities on prohibited lists should be reported to the SCSS and relevant authority within 24 hours prior to departure.

Security procedures

Written procedures must exist for screening business partners, which identify specific factors or practices, the presence of which would trigger additional scrutiny by the exporter.

For those business partners eligible for C-TPAT certification (importers, carriers, ports, terminals, brokers, consolidators, etc.) the exporter must have documentation (e.g., SVI number) indicating whether these business partners are or are not C-TPAT certified and/or participating in a reciprocal Authorized Economic Operator (AEO) program (e.g., AEO certificate).

For those business partners not eligible for C-TPAT certification or participation in an AEO program, exporters must require their business partners to demonstrate that they are meeting C-TPAT security criteria via 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 AEO security program administered by a foreign customs authority; or, by providing a completed exporter security questionnaire). Based upon a documented risk assessment process, non-CTPAT eligible business partners must be subject to verification of compliance with C-TPAT security criteria by the exporter.

Risk assessments of the company's export program must be completed on an annual basis.

Point of Origin

Exporters must inform business partners of security processes and procedures that are consistent with the C-TPAT security criteria to enhance the integrity of the shipment at point of export.

Periodic reviews of business partners' processes and facilities should be conducted based on risk to maintain the security standards required by the exporter.

Participation/Certification in Foreign Customs Administrations Supply Chain Security

Programs:

Current or prospective business partners who have obtained a certification in a supply chain security program being administered by foreign Customs Administration should be required to indicate their status of participation to the exporter.

Other Internal Criteria for Selection

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 exporter.

Internal requirements should be assessed by management utilizing a risk-based document.

Container Security

Container integrity must be maintained to protect against the introduction of unauthorized material and/or persons.

At point of stuffing, written procedures must be in place to properly seal and maintain the integrity of the shipping containers.

Container Inspection

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. A seven-point inspection process is recommended for all containers:

- Front wall
- Left side
- Right side
- Floor
- Ceiling/Roof
- Inside/outside doors, door hardware, and fasteners
- Outside/Undercarriage

Container Seals

The sealing of export containers, to include continuous seal integrity, are crucial elements of a secure supply chain, and remains a critical part of an exporter's commitment to C-TPAT.

A high security seal must be affixed to all loaded containers destined for export from the U.S.

All seals must meet or exceed the current ISO 17712 standards for high security seals.

Written procedures must stipulate how seals are to be controlled and affixed to loaded export containers to include procedures for recognizing and reporting compromised seals and/or containers to CBP or the appropriate foreign authority.

Only designated employees should distribute seals for integrity purposes.

Container Storage

Containers must be stored in a secure area to prevent unauthorized access and/or manipulation and to ensure container integrity is being maintained, especially to protect against the introduction of unauthorized material.

Procedures must be in place for reporting and neutralizing unauthorized entry into containers or container storage areas and any structural changes, such as a hidden compartment, discovered in containers destined for export. Notification should be made within 24 hours of discovery to the assigned Supply Chain Security Specialist (SCSS).

Conveyance Tracking and Monitoring Procedures

Exporters should ensure that their transportation providers adhere to the following tracking and monitoring procedures:

Conveyance and container integrity is maintained while the conveyance is en route transporting cargo to the point of export. Utilizing a tracking and monitoring activity log or equivalent technology is required. If driver logs are utilized, they should reflect that trailer/container integrity was verified.

Predetermined routes should be identified by the transportation provider for the exporter, and these procedures should consist of random route checks by the transportation provider along with documenting and verifying the length of time between the loading point/trailer pickup, the export point, and/or the delivery destinations, during peak and non-peak times.

Drivers should notify the dispatcher of any route delays due to weather, traffic and/or rerouting.

Transportation provider management must perform a documented, periodic, and unannounced verification process to ensure the logs are maintained and conveyance tracking and monitoring procedures are being followed and enforced.

Drivers must report and should document any anomalies or unusual structural modifications found on the conveyance or container.

Physical Access Controls

Access controls prevent unauthorized entry to cargo facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, service providers and vendors at all points of entry. Employees and service providers should only have access to those areas of a facility where they have legitimate business.

Employees: An employee identification system must be in place for positive identification and access control purposes. Employees should only be given access to those secure areas needed for the performance of their duties. Company management or security personnel must adequately control the issuance and removal of employee, visitor and vendor identification

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

Visitors/Vendors/Service Providers: Visitors must present photo identification for documentation purposes upon arrival. All visitors should be escorted and provided temporary identification that must be visibly displayed on their person.

Challenging and Removing Unauthorized Persons: Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.

Deliveries (including mail):

Proper ID and/or photo identification must be presented for documentation purposes upon arrival by transportation providers. Arriving packages and mail should be periodically screened before being disseminated.

Personnel Security

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

Pre-Employment Verification: Application information, such as employment history and references must be verified prior to employment.

Background checks / investigations: Consistent with, federal, state, and local regulations, background checks and investigations should be conducted for prospective employees. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.

Personnel Termination Procedures: Companies must have procedures in place to remove identification, facility, and system access for terminated employees.

Procedural Security

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.

Security procedures should be implemented that restrict access to the export shipment. The procedures should prevent the lading of contraband while en-route from facilities in domestic locations prior to export from the United States.

Cargo Discrepancies: All shortages, overages, and other significant discrepancies or anomalies must be resolved and or investigated appropriately.

Customs, the assigned Supply Chain Security Specialist and or other appropriate law enforcement agencies, must be notified if illegal or suspicious activities are detected-as appropriate.

Documentation Processing: Procedures must be in place to ensure that all information used in the preparation of merchandise/cargo for export (EEI or other required export form), is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous information. Documentation control must include safeguarding computer access and information.

Bill of Lading/Airway Bill/Manifesting Procedures: To help ensure the integrity of cargo being exported, procedures must be in place to ensure that information transmitted/received to/from business partners is reported accurately and timely.

Shipping: The export cargo should be accurately described, and the weights, labels, marks and piece count indicated and verified. Departing cargo should be verified against purchase or delivery orders. Drivers delivering or receiving cargo must be positively identified before cargo is received or released.

Screening for Prohibited or Restricted Parties: Documentable procedures and processes must exist to identify any party on lists from State/DDTC, Commerce/BIS or Treasury/OFAC denied persons and who are involved in an export transaction with the exporter. Entities on prohibited lists should be reported to the SCSS and relevant authority within 24 hours prior to departure.

Physical Security

Procedures must be in place to prevent, detect, or deter undocumented material and unauthorized personnel from gaining access to conveyance, including concealment in containers.

Cargo handling and storage facilities in domestic locations should have physical barriers and deterrents that guard against unauthorized access. Exporters should, according to their business models, incorporate the following C-TPAT physical security criteria throughout their supply chains as practical and appropriate.

Fencing: Perimeter fencing should enclose the areas around cargo handling and storage facilities. Interior fencing within a cargo handling structure should be used to segregate domestic, international, high value, and hazardous cargo. All fencing must be regularly inspected for integrity and damage.

Gates and Gate Houses: Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety.

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

Building Structure: Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.

Locking Devices and Key Controls: All external and internal windows, gates and fences must be secured with locking devices. Management or security personnel must control the issuance of all locks and keys.

Lighting: Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas.

Alarms Systems & Video Surveillance Cameras: Alarm systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas.

Export Training and Threat Awareness

A C-TPAT Exporter must have a documented export security program as well as a designated officer or manager who will act as the C-TPAT program point of contact. This program should have support throughout the corporate structure of the company displayed in correspondence to personnel.

A threat awareness program should be established and maintained to recognize and foster awareness of the threat posed by illegal activities at each point in the supply chain, to include final point of export. There should be documented procedures on how the export security officer or manager receives information about changes in regulations or procedures.

Employees must be made aware of the procedures the company has in place to address a security incident or suspicion thereof and how to report it.

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

Additionally, specific training should be offered to assist employees in maintaining cargo integrity, recognizing internal conspiracies, protecting access controls and enhancing physical security.

These programs should offer incentives for active employee participation.

Information Technology Security

Password Protection: Automated systems must use individually assigned accounts that require a periodic change of password. IT security policies, procedures and standards must be in place and provided to employees in the form of training.

Accountability: A system must be in place to identify the abuse of IT including improper access, tampering or the altering of business data. All system violators must be subject to appropriate disciplinary actions for abuse.