

## C-TPAT Requirements

Dated: June 9<sup>th</sup>, 2009

To: Valued Suppliers

Re: C-TPAT Security Recommendations and Requirements

---

Recently, our company was accepted by US Customs into the C-TPAT program. This program is a joint government-business initiative which helps develop, enhance, and maintain effective security processes throughout the global supply chain. C-TPAT recognizes that Customs can provide the highest level of security only through close cooperation with the ultimate owners of the supply chain, importers, carriers, brokers, warehouse operators, and manufacturers. Through this initiative, Customs is asking businesses to ensure the integrity of their security practices and communicate their security guidelines to their business partners within the supply chain. This program offers businesses an opportunity to play an active role in the war against terrorism. By participating in this first worldwide supply chain security initiative, companies will ensure a more secure supply chain for their employees, suppliers, and customers.

Depending on your role as either a supplier or a transportation provider for one of our companies, please find below our security recommendations as set forth by US Customs & Border Protection ([http://www.cbp.gov/xp/cgov/trade/cargo\\_security/ctpat/](http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/)):

### Quick Click Links

[C-TPAT for Importers](#)

[C-TPAT for Licensed Customs Brokers](#)

[C-TPAT for Foreign Manufacturers](#)

[C-TPAT for Warehouses](#)

[C-TPAT for Air Carriers](#)

[C-TPAT for Ocean Carriers](#)

[C-TPAT for Land Carriers](#)

[Air Freight Consolidators / Ocean Transportation Intermediaries, and NVOCCS](#)

### **I. Importer Security Recommendations for C-TPAT**

Develop and implement a sound plan to enhance security procedures throughout your supply chain. Where an importer does not control a facility, conveyance or process subject to these recommendations, the importer agrees to make every reasonable effort to secure compliance by the responsible party. The following are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

**Procedural Security:** Procedures should be in place to protect against unmanifested material being introduced into the supply chain. Security controls should include the supervised introduction/removal of cargo, the proper marking, weighing, counting and documenting of cargo/cargo equipment verified against manifest documents, the detecting/reporting of shortages/overages, and procedures for verifying seals on containers, trailers, and railcars. The movement of incoming/outgoing goods should be monitored. Random, unannounced security assessments of areas in your company's control within the supply chain should be conducted. Procedures for notifying Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected, or suspected, by the company should also be in place.

**Physical Security:** All buildings and rail yards should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include perimeter fences, locking devices on external and internal doors, windows, gates and fences, adequate lighting inside and outside the facility, and the segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged or otherwise fenced-in area.

**Access Controls:** Unauthorized access to facilities and conveyances should be prohibited. Controls should include positive identification all employees, visitors, and vendors. Procedures should also include challenging unauthorized/unidentified persons.

**Personnel Security:** Companies should conduct employment screening and interviewing of prospective employees to include periodic background checks and application verifications.

**Education and Training Awareness:** A security awareness program should be provided to employees including the recognition of internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should offer incentives for active employee participation in security controls.

**Manifest Procedures:** Companies should ensure that manifests are complete, legible, accurate, and submitted in a timely manner to Customs.

**Conveyance Security:** Conveyance integrity should be maintained to protect against the introduction of unauthorized personnel and material. Security should include the physical search of all readily accessible areas, the securing of internal/external compartments and panels, and procedures for reporting cases in which unauthorized personnel, unmanifested materials, or signs of tampering, are discovered.

## II. Licensed Customs Broker – Security Recommendations for C-TPAT

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

**Procedural Security:** Companies should notify Customs and other law enforcement agencies whenever anomalies or illegal activities related to security issues are detected or suspected.

**Documentation Processing:** Brokers should make their best efforts to ensure that all information provided by the importer/exporter, freight forwarder, etc., and used in the clearing of merchandise/cargo, is legible and protected against the exchange, loss or introduction of erroneous information. Documentation controls should include, where applicable, procedures for:

- Maintaining the accuracy of information received, including the shipper and consignee name and address, first and second notify parties, description, weight, quantity, and unit of measure (i.e. boxes, cartons, etc.) of the cargo being cleared.
- Recording, reporting, and/or investigating shortages and overages of merchandise/cargo.
- Safeguarding computer access and information.

**Personnel Security:** Consistent with federal, state, and local regulations and statutes, companies should establish an internal process to screen prospective employees, and verify employment applications. Such an internal process could include background checks and other tests depending on the particular employee function involved.

**Education and Training Awareness:** A security awareness program should include notification being provided to Customs and other law enforcement agencies whenever anomalies or illegal activities related to security are detected or suspected. These programs should provide:

- Recognition for active employee participation in security controls.
- Training in documentation fraud and computer security controls.

## III. C-TPAT Foreign Manufacturer Security Recommendations

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case by case basis depending on the company's size and structure and may not be applicable to all. The company should have a written security procedure plan in place that addresses the following:

**Physical Security:** All buildings should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include:

- Adequate locking devices for external and internal doors, windows, gates, and fences.
- Segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged, or otherwise fenced-in area.
- Adequate lighting provided inside and outside the facility to include parking areas.
- Separate parking area for private vehicles separate from the shipping, loading dock, and cargo areas.
- Having internal/external communications systems in place to contact internal security personnel or local law enforcement police.

**Access Controls:** Unauthorized access to the shipping, loading dock and cargo areas should be prohibited. Controls should include:

- The positive identification of all employees, visitors and vendors.
- Procedures for challenging unauthorized/unidentified persons.

**Procedural Security:** Measures for the handling of incoming and outgoing goods should include the protection against the introduction, exchange, or loss of any legal or illegal material. Security controls should include:

- Having a designated security officer to supervise the introduction/removal of cargo.
- Properly marked, weighed, counted, and documented products.
- Procedures for verifying seals on containers, trailers, and railcars.
- Procedures for detecting and reporting shortages and overages.
- Procedures for tracking the timely movement of incoming and outgoing goods.
- Proper storage of empty and full containers to prevent unauthorized access.
- Procedures to notify Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the company.

**Personnel Security:** Companies should conduct employment screening and interviewing of prospective employees to include periodic background checks and application verifications.

**Education and Training Awareness:** A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining product integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

#### **IV. C-TPAT Warehouse Security Recommendations**

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all. Warehouses as defined in this guideline are facilities that are used to store and stage both Customs bonded and non-bonded cargo. The company should have a written security procedure plan in place addressing the following:

**Physical Security:** All buildings should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include:

- Adequate locking devices for external and internal doors, windows, gates and fences.
- Adequate lighting provided inside and outside the facility to include parking areas.
- Segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged, or otherwise fenced-in area.
- Separate parking area for private vehicles separate from the shipping, loading dock, and cargo areas.
- Having internal/external communications systems in place to contact internal security personnel or local law enforcement police.

**Access Controls:** Unauthorized access to facilities should be prohibited. Controls should include:

- The positive identification of all employees, visitors, and vendors.
- Procedures for challenging unauthorized/unidentified persons.

**Procedural Security:** Procedures should be in place to protect against unmanifested material being introduced into the warehouse. Security controls should include:

- Having a designated security officer to supervise the introduction/removal of cargo.
- Properly marked, weighed, counted, and documented cargo/cargo equipment verified against manifest documents.
- Procedures for verifying seal on containers, trailers, and railcars.
- Procedures for detecting and reporting shortages and overages.
- Procedures to notify Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the company.
- Proper storage of empty and full containers to prevent unauthorized access.

**Personnel Security:** Companies should conduct employment screening and interviewing of prospective employees to include periodic background checks and application verifications.

**Education and Training Awareness:** A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

## V. Air Carrier Security Recommendations for C-TPAT

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

**Conveyance Security:** Aircraft integrity should be maintained to protect against the introduction of unauthorized personnel and material. Conveyance security procedures should include the physical search of all readily accessible areas, securing all internal/external compartments and panels, and reporting cases in which unmanifested materials, or signs of tampering, are discovered.

**Access Controls:** Unauthorized access to the aircraft should be prohibited. Controls should include the positive identification of all employees, visitors and vendors as well as procedures for challenging unauthorized/unidentified persons.

**Procedural Security:** Procedures should be in place to protect against unmanifested material being introduced aboard the aircraft. Security controls should include complete, accurate and advanced lists of international passengers, crews, and cargo, as well as a positive baggage match identification system providing for the constant security of all baggage. All cargo/cargo equipment should be properly marked, weighed, counted, and documented under the supervision of a designated security officer. There should be procedures for recording, reporting, and/or investigating shortages and overages, and procedures to notify Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the carrier.

**Manifest Procedures:** Companies should ensure that manifests are complete, legible, accurate, and submitted in a timely manner to Customs.

**Personnel Security:** Employment screening, application verifications, the interviewing of prospective employees and periodic background checks should be conducted.

**Education and Training Awareness:** A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

**Physical Security:** Carrier's buildings, warehouses, and on & off ramp facilities should be constructed of materials which resist unlawful entry and protect against outside intrusion. Physical security should include adequate locking devices for external and internal doors, windows, gates and fences. Perimeter fencing should also be provided, as well as adequate lighting inside and outside the facility; including parking areas. There should also be segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by means of a safe, cage, or otherwise fenced-in area.

## **VI. Ocean Carrier Security Recommendations for C-TPAT**

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

**Conveyance Security:** Vessel integrity should be maintained to protect against the introduction of unauthorized personnel and material. Conveyance security should include the physical search of all readily accessible areas, the securing all internal/external compartments and panels as appropriate, and procedures for reporting cases in which unmanifested materials, or signs of tampering, are discovered.

**Access Controls:** Unauthorized access to the vessel should be prohibited. Controls should include the positive identification of all employees, visitors, and vendors. Procedures for challenging unauthorized/unidentified persons should be in place.

**Procedural Security:** Procedures should be in place to protect against unmanifested material being introduced aboard the vessel. Security procedures should provide for complete, accurate and advanced lists of crews and passengers. Cargo should be loaded and discharged in a secure manner under supervision of a designated security representative and shortages/overages should be reported appropriately. There should also be procedures for notifying Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected, or suspected, by the company.

**Manifest Procedures:** Manifests should be complete, legible, accurate and submitted in a timely manner pursuant to Customs regulations.

**Personnel Security:** Employment screening, application verifications, the interviewing of prospective employees and periodic background checks should be conducted.

**Education and Training Awareness:** A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

**Physical Security:** Carrier's buildings should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include adequate perimeter fencing, lighting inside and outside the facility, and locking devices on external and internal doors, windows, gates, and fences.

## **VII. Land Carrier Security Recommendations for C-TPAT**

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

**Conveyance Security:** Integrity should be maintained to protect against the introduction of unauthorized personnel and material. Conveyance security procedures should include the physical search of all readily accessible areas, securing all internal/external compartments and panels, and procedures for reporting cases in which unmanifested materials, or signs of tampering, are discovered.

**Physical Security:** All carrier buildings and rail yards should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include adequate locking devices on external and internal doors, windows, gates and fences. Perimeter fencing should be addressed, as well as adequate lighting inside and outside the facility, to include the parking areas. There should be segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged or otherwise fenced-in area.

**Access Controls:** Unauthorized access to facilities and conveyances should be prohibited. Controls should include the positive identification of all employees, visitors, and vendors as well as procedures for challenging unauthorized/unidentified persons.

**Procedural Security:** Procedures should be in place to protect against unmanifested material being introduced aboard the conveyance. Security controls should include the proper marking, weighing, counting, and documenting of cargo/cargo equipment under the supervision of a designated security representative. Procedures should be in place for verifying seals on containers, trailers, and railcars, and a system for detecting and reporting shortages and overages. The timely movement of incoming and outgoing goods should be tracked and there should be procedures for notifying Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the company.

**Manifest Procedures:** Companies should ensure that manifests are complete, legible, accurate, and submitted in a timely manner to Customs.

**Personnel Security:** Companies should conduct employment screening and interviewing of prospective employees to include periodic background checks and application verifications.

**Education and Training Awareness:** A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

#### **VIII. Air Freight Consolidators / Ocean Transportation Intermediaries, and NVOCCS Security Recommendations for C-TPAT**

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

**Procedural Security:** Companies should notify Customs and other law enforcement agencies whenever anomalies or illegal activities related to security issues are detected or suspected.

**Documentation Processing:** Consolidators should make their best efforts to ensure that all information provided by the importer/exporter, freight forwarder, etc., and used in the clearing of merchandise/cargo, is legible and protected against the exchange, loss or introduction of erroneous information. Documentation controls should include, where applicable, procedures for:

- Maintaining the accuracy of information received, including the shipper and consignee name and address, first and second notify parties, description, weight, quantity, and unit of measure (i.e. boxes, cartons, etc.) of the cargo being cleared.
- Recording, reporting, and/or investigating shortages and overages of merchandise/cargo.
- Tracking the movement of incoming and outgoing cargo.
- Safeguarding computer access and information.

Companies should participate in the Automated Manifested System (AMS) and all data submissions should be complete, legible, accurate and submitted in a timely manner pursuant to Customs regulations.

**Personnel Security:** Consistent with federal, state, and local regulations and statutes, companies should establish an internal process to screen prospective employees, and verify applications. Such an internal process could include background checks and other tests depending on the particular employee function involved.

**Education and Training Awareness:** A security awareness program should include notification being provided to Customs and other law enforcement agencies whenever anomalies or illegal activities related to security are detected or suspected. These programs should provide:

- Recognition for active employee participation in security controls.
- Training in documentation fraud and computer security controls.