A Message Regarding Security Procedures Guidelines for

# Manufacturers and Suppliers

Outside the United States

Tricar Sales Inc. is a participant in the Customs-Trade Partnership Against Terrorism (CTPAT) program of the United States Customs & Border Patrol agency (CBP).

CTPAT is a voluntary joint government-business initiative to build cooperative relationships that strengthen the overall supply chain and border security. Everyone involved in logistics, distribution, or supply chain management will be impacted by ongoing efforts to create a more secure global trading system. **The CTPAT program is similar to Authorized Economic Operator (AEO) security programs in many other countries around the world.**

Importers such as our company are expected to complete a security assessment of our entire supply chain. The assessment must include the security-related subjects of:

Access Control
Agricultural Procedures
Business Partners
Conveyance Security
Information Technology
Personnel Security
Physical Security
Procedural Security
Security Awareness Training
Trade-Based Money Laundering
Upper Management Responsibility

As our business partner, it is necessary for your company to have and continuously seek to improve upon security processes and procedures consistent with CTPAT security criteria. Hence, we request that you provide one (only) of the following documents to verify compliance with CTPAT security-procedures guidelines.

− Copy of CTPAT Certification (only for CTPAT certified companies). − Certification of participation in a foreign Customs security program. − Documentation from a corporate officer attesting to compliance. − Completion of a security questionnaire for your industrial sector.

Please provide this information to us as soon as you receive this letter. If you should have any questions, please contact us by replying to the email by which you received this message, or at telephone number: (520)377-7601

Thank you for your assistance with this very important matter.

Best regards, Tricar Sales Inc.

# CTPAT Security Procedures Guidelines for

# **Manufacturers and Suppliers**

# Outside the United States

These following minimum-security criteria are designed for foreign (non-U.S.) manufacturers to create or verify effective security practices designed to optimize supply-chain performance by eliminating theft, loss, contraband smuggling, trade-based money laundering and the introduction of terrorism and other crime into the global supply chain.

Periodically, foreign manufacturers must assess their international supply chains based upon the below security criteria. Where a foreign manufacturer or supplier outsources or contracts elements of their supply chain, such as another foreign facility, warehouse, or other elements, the foreign manufacturer must work with these business partners to ensure that their related security measures are in place and are adhered to throughout their supply chain. The supply chain for these security-procedures purposes is defined as from point of origin (manufacturer/supplier/vendor) through to point of distribution.

CTPAT recognizes the complexity of international supply chains and security practices and endorses the application and implementation of security measures based upon risk. Therefore, the program allows for flexibility and the customization of security plans based on the member's business model. However, appropriate security measures such as listed throughout this document must be implemented and maintained.

## Business Partner Requirement

Foreign manufacturers and their business partners must have written and verifiable processes (SOPs) for the selection of business partners including other manufacturers, product suppliers, carriers, consolidators and other vendors (parts and raw material suppliers, etc.).

### Security procedures verification

The business partners of the foreign manufacturer must demonstrate that they and their business partners are meeting CTPAT security criteria via written/electronic confirmation (for example, 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 CTPAT security criteria or an equivalent World Customs Organization (WCO) accredited security program administered by their foreign customs authority; or, by providing a completed security questionnaire).

### Point of Origin

Foreign manufacturers must ensure that business partners develop security processes and procedures consistent with the CTPAT security criteria to enhance the integrity of the shipment at point of origin, assembly, or manufacturing. Periodic reviews of business partners' processes and facilities should be conducted based on risk and should maintain the security standards required by the foreign manufacturer.

**Security Procedures**
On U.S. bound shipments, foreign manufacturers should monitor that carriers that subcontract transportation services to other carriers use approved security criteria as outlined in these business-partner requirements.

As the foreign manufacturer is responsible for loading trailers and containers, they should work with carriers and consolidators to provide reassurance that there are effective security procedures and controls implemented during all periods of transportation and at the point-of-stuffing.

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

In those geographic areas where risk assessments warrant checking containers or trailers for human concealment or smuggling, such procedures should be designed to address this risk at the manufacturing facility or point-of-stuffing.

**Container Inspection**
Procedures must be in place to verify the physical integrity of a shipping-container's 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
- Outside/Undercarriage

**Trailer Inspection**
Procedures must be in place to verify the physical integrity of the trailer structure prior to stuffing, to include the reliability of the locking mechanisms of the doors. The following five-point inspection process is recommended for all trailers:

- Fifth wheel area - check natural compartment/skid plate
- Exterior - front/sides
- Rear - bumper/doors
- Front wall
- Left side

### Container and Trailer Seals

The sealing of trailers and containers, to include continuous seal integrity, are crucial elements of a secure supply chain, and remains a critical part of a foreign manufacturers' commitment to security procedures. The foreign manufacturer must affix a high security seal to all loaded trailers and containers bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standards for high security seals.

Written procedures must stipulate how seals are to be both controlled in storage and  affixed to loaded containers and trailers, to include procedures for recognizing and reporting compromised seals and/or containers/trailers to US Customs and Border Protection or the appropriate foreign authority. Only designated employees should distribute seals for integrity purposes.

### Container and Trailer Storage

Containers and trailers under foreign manufacturer control or located in a facility of the foreign manufacturer must be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting and neutralizing unauthorized entry into containers/trailers or container/trailer storage areas.

## Physical Access Controls

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.

### 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 (for example, keys, key cards, etc.) must be documented.

### Visitors

Visitors must present photo identification for documentation purposes upon arrival. All visitors should be escorted and should visibly display temporary identification.

### Deliveries (including mail)

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

### Challenging and Removing Unauthorized Persons

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

## 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 foreign 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.

### Documentation Processing

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. Documentation control must include safeguarding computer access and information.

### Manifesting Procedures

To help ensure the integrity of cargo, procedures must be in place to ensure that information received from business partners is reported accurately and in a timely manner.

### Shipping and Receiving

Departing cargo being shipped should be reconciled against information on the cargo manifest. The 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. Procedures should also be established to track the timely movement of incoming and outgoing goods.

### Cargo Discrepancies

All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. Customs and/or other appropriate law enforcement agencies must be notified if anomalies, illegal or suspicious activities are detected - as appropriate.

## Physical Security

Cargo handling and storage facilities in international locations must have physical barriers and deterrents that guard against unauthorized access. Foreign manufacturer should incorporate the following CTPAT-like physical security criteria throughout their supply chains as applicable.

### 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 and 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.

## Cybersecurity

Manufacturers and their partners must have comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems. The written IT policy, at a minimum, must cover all the individual Cybersecurity criteria below. Information Technology (IT) integrity must always be maintained to protect data from unauthorized access or manipulation.

- **Network Protection**

To defend Information Technology (IT) systems against common cybersecurity threats, a company must install sufficient software/hardware protection from malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewalls) in Members' computer systems. Members must ensure that their security software is current and receives regular security updates. Members must have policies and procedures to prevent attacks via social engineering. If a data breach occurs or another unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and/or data.

- **Testing**

Companies using network systems must regularly test the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.

- **User Access**

User access must be restricted based on job description or assigned duties. Individuals with access to Information Technology (IT) systems must use individually assigned accounts. Authorized access must be reviewed on a regular basis to ensure access to sensitive systems is based on job requirements. Computer and network access must be removed upon employee separation.

- **Accountability & Identification of Abuse**

A system must be in place to identify unauthorized access of IT systems/data or abuse of policies and procedures including improper access of internal systems or external websites and tampering or altering of business data by employees or contractors. All violators must be subject to appropriate disciplinary actions

- **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 training provided to employees. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication and user access to IT systems must be safeguarded. Passwords and/or passphrases must be changed as soon as possible if there is evidence of compromise or reasonable suspicion of a compromise exists.

- **VPNs**

Members that allow their users to remotely connect to a network must employ secure technologies such as virtual private networks (VPNs) or multi-factor authentication (MFA) to allow employees to access the company's intranet securely when located outside of the office. Members must also have procedures designed to prevent remote access from unauthorized users.

- **Data**

Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format.

### Security Training and Threat Awareness

A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by terrorists and contraband smugglers at each point in the supply chain. Employees must be made aware of the procedures the company has in place to address a situation and how to report it. Additional training should be provided to employees in 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, and protecting access controls. These programs should offer incentives for active employee participation.

### Trade-Based Money Laundering

Trade-Based Money Laundering occurs when criminals use the international trade system to disguise illicit proceeds by altering Customs and banking paperwork to make transactions appear legitimate. These proceeds are then used to finance additional criminal activity, which may include funding terrorist activities or organizations.

Manufacturers and their business partners must have a written, risk-based process for screening new business partners and for monitoring current partners. A factor that Members should include in this process is checks on activity related to money laundering and criminal funding as there is a marked overlap between the two. Specialized training should be provided annually to personnel who may be able to identify the warning indicators of Trade-Based Money Laundering and Terrorism Financing (examples of personnel who should receive this training include those responsible for trade compliance, security, procurement, finance, shipping, and receiving).

To assist with this process, please consult the document CTPAT's Warning Indicators for Trade-Based Money Laundering and Terrorism Financing Activities, as found on the Tricar Sales web site or as provided on the internet at the U.S. Customs and Border Patrol CTPAT program website.

The following are examples of some of the vetting elements that can help determine if a company is legitimate:

- Verifying the company's business address and how long they have been at that address.
- Conducting research on the internet on both the company and its principals.
- Checking business references.
- Requesting a credit report.

### Upper Management Responsibility

The role of a company's upper management in CTPAT is to provide support and oversight to ensure the creation and maintenance of the company's Supply Chain Security Program. To this end, the designated company CTPAT administrator, head of security, or security coordinator should provide regular updates regarding the progress or outcomes of any audits, exercises, or validations to upper management.

To promote a culture of security, a letter of commitment to supply chain security (and/or the CTPAT program) should be signed by a senior company official and displayed in appropriate company locations.

### Wood Packaging Materials, Pallets (Agricultural Procedures)

Visible pest contamination is to include compliance with Wood Packaging Materials (WPM) regulations. Measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15). This is a firm requirement of CTPAT as visible pest prevention measures must be adhered to throughout the supply chain.

[end document]

CERTIFICATION COORDINATOR