



**MARTIN E. BUTTON, INC.**  
Cosdel International Transportation  
55 New Montgomery Street, Suite 400  
San Francisco, CA 94105  
Phone:(415)777-2000 Fax:(415)543-5112

Dear Valued Business Partner:

The U.S. Bureau of Customs and Border Protection (Customs) is sponsoring the **Customs-Trade Partnership against Terrorism (C-TPAT)** program. C-TPAT is a joint government business initiative to build cooperative relationships that strengthen the security of the supply chain. The direct benefit to participants is a shortened import cycle time and fewer Customs cargo examinations. Martin E. Button, Inc. is a participant in C-TPAT.

C-TPAT requires brokers conduct a comprehensive assessment of their international supply chains based upon C-TPAT security guidelines. Where a broker out sources or contracts elements of their supply chain, such as a foreign facility, conveyance, domestic warehouse, or other elements, the broker must work with these business partners to ensure that pertinent security measures are in place and adhered to throughout their supply chain.

Please demonstrate your company meets C-TPAT security guidelines by completing the questionnaire below. Please return the questionnaire to my attention at your earliest convenience.

You can find detailed C-TPAT information on Customs web site at [www.cbp.gov](http://www.cbp.gov). Click on "*Customs - Trade Partnership Against Terrorism (C-TPAT)*" link.

We appreciate your cooperation as we work to contribute to safe and secure international trade while managing our costs and cycle time. If you have any questions, please call me at above phone number.

With Kind Regards,

Martin E. Button, Inc.



**MARTIN E. BUTTON, INC.**  
 Cosdel International Transportation  
 55 New Montgomery Street, Suite 400  
 San Francisco, CA 94105  
 Phone:(415)777-2000 Fax:(415)543-5112

***Martin E. Button, Inc. Business Partner Security Questionnaire***

Name: \_\_\_\_\_

Years in Business \_\_\_\_\_

Address \_\_\_\_\_

Number of Employees \_\_\_\_\_

\_\_\_\_\_

Contact Party: \_\_\_\_\_

E-mail \_\_\_\_\_

Phone: \_\_\_\_\_

Fax \_\_\_\_\_

Other Name(s) Your Company Uses \_\_\_\_\_

Business Partner Type: (Please circle one)

Agent

Carrier

Custom Broker

Freight Forwarder

NVOCC

Importer

Manufacturer

Warehouse

Other \_\_\_\_\_

C-TPAT Certification Status: Yes                      No                      C-TPAT Member SVI# \_\_\_\_\_

Date of Certification: \_\_\_\_\_

Please attach copy of C-TPAT certificate or acceptance letter

\_\_\_\_ Applied, but certification not received

\_\_\_\_ Application for C-TPAT is in process

\_\_\_\_ No plans for C-TPAT

\_\_\_\_ Others, please specify \_\_\_\_\_

**IF YOU HAVE INDICATED THAT YOU ARE A C-TPAT MEMBER, PROCEED DIRECTLY TO "CERTIFICATION"**

As a C-TPAT participant, we must conduct a comprehensive assessment of our international supply chain based upon C-TPAT security criteria. Where Martin E. Button, Inc. outsources or contracts elements of their supply chain, such as a foreign facility, conveyance, domestic warehouse, or other element, we must work with these business partners to ensure that pertinent security measures are in place and adhered to throughout the supply chain. The supply chain for C-TPAT purposes is defined from point of origin through to point of distribution.

**Please answer the questions below**

### Business Partner Requirements

#### **Point of Origin**

Has your company developed security processes and procedures consistent with the C-TPAT security criteria to enhance the integrity of shipments at their point of origin? Yes No

#### **Participation / Certification in Foreign Customs Administrations Supply Chain Security Programs**

Does your company monitor the participation of current or prospective business partners in supply chain security programs administered by foreign Customs? Yes No

#### **Container Security**

Does your company have procedures in place to properly seal and maintain the integrity of shipping containers at the point of stuffing? Yes No

#### **Container Inspection**

Do you have procedures 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? Yes No

We recommend a seven-point inspection process (as follows) for all containers:

- Front wall
- Left side
- Right side
- Floor
- Ceiling/Roof
- Inside/outside doors
- Outside/Undercarriage

#### **Container Seals**

*Only designated employees should distribute container seals. This maintains integrity in their use.*

Do you have written procedures stipulating how seals are to be controlled and affixed to loaded containers - to include procedures for recognizing and reporting compromised seals and/or containers to US Customs and Border Protection or the appropriate foreign authority? Yes No

#### **Container Storage**

Are containers stored in a secure area to prevent unauthorized access and/or manipulation? Yes No

Do you have procedures in place for reporting and neutralizing unauthorized entry into containers or container storage areas? Yes No

#### **Physical Access Controls**

Does your company have access controls prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets? Yes No

Does your company's access controls include the positive identification of all employees, visitors, and vendors at all points of entry? Yes No

**Employees**

Do you have an employee identification system in place for positive identification and access control purposes? Yes No

*Are employees only given access to those secure areas needed for the performance of their duties?* Yes No

Do company management or security personnel adequately control the issuance and removal of employee, visitor and vendor identification badges? Yes No

Are procedures for the issuance, removal and changing of access devices (e.g. access keys etc.) documented? Yes No

**Visitors**

Do visitors present photo identification for documentation purposes upon arrival? Yes No

*Are visitors escorted and do they visibly display temporary identification?* Yes No

**Deliveries (including mail)**

Is proper vendor ID and/or photo identification presented for documentation purposes upon arrival by all vendors? Y N

*Are arriving packages and mail periodically screened before being disseminated?* Yes No

**Challenging and Removing Unauthorized Persons**

Are procedures in place to identify, challenge and address unauthorized/unidentified persons? Yes No

**Personnel Security**

Are processes in place to screen prospective employees and to periodically check current employees? Yes No

**Pre-Employment Verification**

Is application information, such as employment history and references verified prior to employment? Yes No

**Background checks / investigations**

*Do you, consistent with foreign, federal, state, and local regulations, conduct background checks and investigations for prospective employees?* Yes No

*Once employed, are periodic checks and reinvestigations performed based on cause, and/or the sensitivity of the employee's position?* Yes No

**Personnel Termination Procedures**

Are procedures in place to remove identification, facility, and system access for terminated employees? Yes No

**Procedural Security**

Are security measures in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain? Yes No

**Documentation Processing**

Are procedures 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? Yes No

Does documentation control include safeguarding computer access and information? Yes No

### Security Training and Threat Awareness

Are employees made aware of the procedures the company has in place to address a situation and how to report it? Yes No

*Is additional training provided to employees in the shipping and receiving areas, as well as those receiving and opening mail?* Yes No

*Do you offer specific training to assist employees in maintaining cargo integrity, recognizing internal conspiracies, and protecting access controls?* Yes No

*Do you offer incentives for active employee participation in these programs?* Yes No

### Physical Security

Do cargo handling and storage facilities have physical barriers and deterrents that guard against unauthorized access? Yes No

**Fencing** (All fencing must be regularly inspected for integrity and damage.)  
*Does perimeter fencing enclose the areas around cargo handling and storage facilities?* Yes No

*Is Interior fencing within a cargo handling structure used to segregate domestic, international, high value, and hazardous cargo?* Yes No

### Gates and Gate Houses

Are gates through which vehicles and/or personnel enter or exit manned and/or monitored? Yes No

### Parking

Are private passenger vehicles prohibited from parking in or adjacent to cargo handling and storage areas? Yes No

### Building Structure

Are buildings constructed of materials that resist unlawful entry? Yes No

Is the integrity of structures maintained by periodic inspection and repair? Yes No

### Locking Devices and Key Controls

Are all external and internal windows, gates and fences secured with locking devices? Yes No

Do management or security personnel control the issuance of all locks and keys? Yes No

### Lighting

Is adequate lighting provided inside and outside the facility including the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas? Yes No

### Alarms Systems & Video Surveillance Cameras

*Do you use alarm systems and video surveillance cameras to monitor premises and prevent unauthorized access to cargo handling and storage areas?* Yes No

### Information Technology (IT) Security

#### Password Protection

Are automated systems individually assigned accounts that require a periodic change of password? Yes No

Are IT security policies, procedures and standards in place and provided to employees in the form of training? Yes No

#### Accountability

Is a system in place to identify the abuse of IT including improper access, tampering or the altering of business data? Yes No

Are system violators subject to appropriate disciplinary actions for abuse? Yes No