Boeing Customs-Trade Partnership Against Terrorism (C-TPAT) Security Guidelines for International Suppliers/Shippers

In support of Boeing's C-TPAT program implementation, these security requirements and guidelines are provided to international shippers to institute effective security practices designed to ensure supply chain security to mitigate the risk of loss, theft, and contraband smuggling that could potentially introduce terrorists and implements of terrorism into the global supply chain.

The following security criteria, as outlined by the US Customs and Border Protection (CBP) Customs – Trade Partnership Against Terrorism (C-TPAT) program, identify areas and opportunities for ensuring security of the supply chain supporting Boeing:

1. Business Partnerships/Use of Sub-Contractors

Supplier/Shipper shall ensure that they and any sub-contracted supplier/shipper or logistics service provider involved in handling any shipment being sent directly to the U.S. (for which Boeing is the U.S. Importer of Record) employs security practices which ensure the security of such shipments. If supplier/shipper sub-contracts with other suppliers/shippers or logistics service providers engaged in manufacturing, packaging, or transport of Boeing shipments directly to the U.S., the supplier/shipper must have documented processes for the selection of such business partners to ensure that they are a viable business that will provide adequate supply chain security.

International suppliers/shippers should ensure that any business partners involved in handling shipments to Boeing be knowledgeable of and demonstrate that they are meeting the Boeing C-TPAT Security Guidelines this may be accomplished via written/electronic confirmation (i.e. contractual obligations; via a letter attesting to compliance; a written statement from the business partner demonstrating their compliance with C-TPAT security criteria or an equivalent a supply chain security program sponsored by your nation; or, by providing a completed security questionnaire).

2. Physical Security

Supplier/Shipper facilities must have physical security deterrents that protect against unauthorized access. Physical security deterrents employed by international suppliers/shippers may include, but are not limited to, the following elements:

2.1 Fencing

Perimeter fencing or walls should enclose supplier/shipper facilities where other controls are not in place to prevent unauthorized access. All fencing and walls should be regularly inspected and maintained. Best practices also include internal securing of shipping and receiving areas via fencing, locking doors, or other access controls

2.2 Gates/Entries

Entry and exit points for vehicles and/or personnel must be controlled. The number of gates should be kept to the minimum necessary for proper access and safety controls.

2.3 Guards

Guards or access controls should be in place to ensure that unauthorized personnel do not enter the facility or gain access to Boeing shipments.

2.4 Parking Controls

Private passenger vehicles should be prohibited from parking in or adjacent to shipping and receiving areas to prevent unauthorized materials from being introduced into shipments or conveyance vehicles.

2.5 Locking Devices and Key Controls

External and internal windows, gates, and doors through which unauthorized personnel could access the facility or cargo storage areas must be secured with locking devices. Management or security personnel should control the issuance of all locks and keys.

2.6 Lighting

Adequate lighting must be provided inside and outside the facility to prevent unauthorized access.

2.7 Alarms Systems and Video Surveillance Cameras

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

3. Access Controls

Access controls (e.g. badge readers, locks, key cards, guards, etc.) must prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect Boeing's assets. Access controls should include the positive identification of all employees, visitors, and vendors at all points of entry and use of badges for employees and visitors.

3.1 Employees

An employee identification system must be in place for positive identification and access control purposes. Company management or security personnel must adequately control the issuance and removal of employee, visitor and vendor identification badges.

3.2 Visitors

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

3.3 Access Devices

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

3.4 Deliveries

Proper vendor identification and/or photo identification must be presented upon arrival by all vendors for documentation purposes. Controls should be in place to ensure vendor access is limited to the areas necessary to perform their duties.

3.5 Challenging and Removing Unauthorized Persons

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

4. Personnel Security

Screen prospective employees consistent with local regulations. Verify employment application information prior to employment.

4.1 Background Checks / Investigations

Background checks should be conducted for potential employees. Such checks may include; educational and employment background, criminal records and other information to confirm the identification of potential employees. Once employed, periodic checks should be performed based on cause, and/or the sensitivity of the employee's position.

4.2 Personnel Termination Procedures

Companies must have procedures in place to remove badges, uniforms, and facility and IT system access for terminated employees.

5. Ocean Container and Truck Trailer Security

Container and trailer security must be maintained to protect against the introduction of unauthorized material and/or persons. For suppliers/shippers that stuff/load the ocean container at their facility, procedures must be in place to properly seal and maintain the security of shipping containers and trailers at the point of stuffing. A high security seal must be affixed to all access doors on truck trailers (from Canada or Mexico) and ocean containers bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standard for high security seals.

If the supplier/shipper is not contractually responsible for stuffing / loading the ocean container or getting the cargo to the stuffing location under established Boeing INCOTerms (e.g. ExWorks) and/or agreements, cargo container and trailer security procedures, including bolt seal requirements, the supplier/shipper is not responsible for container and trailer security.

5.1 Ocean Container and Truck Trailer Inspection: If the supplier/shipper is responsible for stuffing ocean containers or truck trailers destined for Boeing, an inspection must be conducted on the ocean container or truck trailer prior to stuffing, including the reliability of the locking mechanisms of the doors. A seven-point inspection process is recommended for all containers:

1. Front wall
2. Left side
3. Right side
4. Floor
5. Ceiling/Roof
6. Inside/outside doors
7. Outside/Undercarriage

For Truck Trailers, these 3 additional inspections are recommended:

8. Fifth wheel area - check natural compartment/skid plate
9. Exterior - front/sides
10. Rear - bumper/doors

5.2 Ocean Container and Truck Trailer Storage: Ocean containers and truck trailers under the supplier's/shipper's control or located in a facility of the supplier/shipper must be stored in a secure area to prevent unauthorized access and/or manipulation.

5.3 Security and Control of Container and Trailer Seals

The international supplier/shipper must affix a high security seal to all fully loaded ocean containers or truck trailers (i.e. from Canada or Mexico) bound for the U.S. when such trailers and containers are stuffed at the supplier's/shipper's location.

International suppliers/shippers must have documented procedures in place to manage, control and record the issuance and use of high security bolt seals. Such procedures should include procedures for recognizing and reporting compromised seals and/or containers/trailers. Only designated employees should distribute and apply seals for security purposes. Best practices include storing seals in a locked area or cabinet, limiting access to select employees, and keeping a documented inventory of all seals.

6. Information Technology (IT) Security

Security measures must be in place to ensure automated systems are protected from unauthorized access.

6.1 Password Protection

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

6.2 Accountability

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

7. Procedural Security

Security procedures must exist, be documented and communicated to employees to ensure the security measures in this document are followed. Common documentation formats include the use of a security manual, policies, employee handbook, or the like. Upon Boeing's request, international supplier/shipper shall provide evidence of such documented procedures. Specific to Boeing shipments, the following procedures must be documented and communicated:

7.1 Procedures for the issuance, removal and changing of access devices.
7.2 Procedures to identify and challenge unauthorized or unidentified persons
7.3 Procedures to remove identification, facility, and system access for terminated employees.
7.4 Procedures for IT security and standards.
7.5 Procedures for employees to report security incidents and/or suspicious behavior.
7.6 Procedures for the inspection of ocean containers or truck trailers prior to stuffing.
7.7 Procedures to manage control and record the issuance and use of high security bolt seals for ocean containers and truck trailers.

7.8 Shipment Documentation Security Procedures

Procedures should be in place to ensure that all information used in the clearing of shipments through Customs is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous information. Documentation control should include safeguarding computer access and information related to Boeing shipments.

7.9 Shipping and Receiving Security Procedures

Procedures should be in place to ensure that departing cargo is verified against purchase or delivery orders. Best practices include a documented process to ensure accurate piece count, weight and part numbers and verification that contraband is not present. Drivers picking up cargo should be positively identified before cargo is released.

7.10 Shipping and Packaging Security Procedures

Documented procedures should be in place to control the access to shipping and packaging areas. Once packaged, all shipments should be securely controlled to prevent unauthorized access and the possible introduction of any contraband items.

8. Security Training

A security training program should be established and maintained to educate and build employee awareness of proper security procedures as outlined in these security guidelines. Best practices include training on the threat posed by terrorists and contraband smugglers at each point in the supply chain as well as training on topics such as ethical conduct, and avoidance of corruption, fraud and exploitation. Additional training on ensuring proper supply chain security should be provided to employees in the shipping and receiving areas.,

A documented procedure must be in place for employees to report any security incidents and/or suspicious behavior.

9. Shipment Routing

International suppliers/shippers shall follow all INCOTerms, routing, and International Shipment Routing Instructions provided by Boeing. If the international supplier/shipper does not control the routing of the goods between the point of origin and the point of delivery to Boeing, the foreign supplier/shipper is not responsible for supply chain security beyond the point of shipment transfer per the INCOTerms.

On U.S. bound Boeing shipments coordinated by the supplier/shipper; international suppliers/shippers shall use transportation freight forwarders and carriers who are either C-TPAT certified or who meet the Boeing C-TPAT Security Guidelines.