Boeing World Customs Organization (WCO) Security Guidelines for International Supply Chain Stakeholders

In support of Boeing's certification in the World Customs Organization's nationally recognized supply chain security programs, these security requirements and guidelines are provided to supply chain stakeholders: international shippers, warehouses, transportation service providers, and customs brokers to institute effective security practices. These practices are designed to ensure supply chain security that mitigates the risk of loss, theft, and introduction of contraband that could potentially disrupt the global supply chain and our business.

Boeing supply chain stakeholders are encouraged to participate in national supply chain security programs including, but not limited to CTPAT, Authorized Economic Operator (AEO), Partners in Protection (PIP), and equivalent programs.

Customs Trade Partnership Against Terrorism

Authorized Economic Operator

Australian Trusted Trader

Partners in Protection

The following security criteria, as outlined by WCO recognized supply chain security programs, identify areas and opportunities for ensuring security of the supply chain supporting Boeing:

1. Business Partnerships/Use of Sub-Contractors

International supply chain stakeholders should ensure that any business partners involved in handling shipments to Boeing be knowledgeable of and demonstrate that they are meeting the Boeing WCO Security Guidelines.

Supply chain stakeholders shall have documented processes for the selection of subcontractors. This process shall ensure that such subcontractors maintain adequate security controls and procedures and verify subcontractor compliance to the identified security controls.

2. Physical Security

Supply chain stakeholders must maintain facilities with physical security deterrents that protect against unauthorized access including, but not limited to, cargo handling and storage facilities. The following physical security deterrents are recommended:

i. 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

ii. 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.

iii. 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.

iv. 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.

v. 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.

vi. Lighting

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

vii. Alarms Systems and Video Surveillance Cameras

Where security technology is utilized (including alarms, access control devices, and video surveillance systems) appropriate and written policies governing the use, maintenance, and protection of such technology must be in place.

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.

i. 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.

ii. Visitors

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

iii. 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.).

viii. 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.

4. Personnel Security

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

i. 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.

ii. 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. Loading/stuffing of cargo should be supervised by a security officer or designated personnel.

i. Ocean Container and Truck Trailer Inspection

Seller will inspect all ocean containers or truck trailers prior to stuffing.

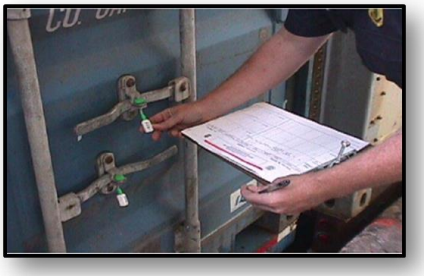
a) Inspections must include:
- Review of the reliability of the locking mechanisms of all doors and external hardware
- Examination for visible agricultural pests
- Confirmation that structures have not been modified to conceal contraband

b) Inspections should be documented on a checklist including:
- Container/Trailer/IIT number
- Date of Inspection
- Time of Inspection
- Name of employee conducting inspection
- Specific areas of the IIT that were inspected
- Signature of personnel supervising the inspection of container

ii. Ocean Container and Truck Trailer Seals

Properly seal and secure shipping containers and trailers at the point of stuffing using the VVTT process (View, Verify, Tug, Twist). Seller will affix a high security seal to all access doors on truck trailers (from Canada or Mexico) and ocean containers bound for the U.S.

a) Seals must meet or exceed the current PAS ISO 17712 standard for high security seals
b) When containers or trailers are picked up or stopped, the seal number must be confirmed to match what is on the shipping documentation
c) If a seal is broken, Seller will immediately notify Boeing and indicate when it was broken, who broke it, and the replacement seal number
d) Any seal broken, altered or tampered with must be held in order to aid investigation



iii. Ocean Container and Truck Trailer Storage

Seller will store empty or stuffed ocean containers and truck trailers in a secure area to prevent unauthorized access and/or manipulation.

6. Conveyance Security

When performing or subcontracting transportation services, conveyance and container integrity shall be maintained while the conveyance is en route transporting cargo from origin to destination, including, but not limited to, tracking and monitoring activity logs, a documented verification process, and driver notification of any abnormalities with the conveyance and/or container.

7. Cybersecurity

Security measures must be in place to ensure automated systems are protected from unauthorized access and cybersecurity threats. Companies are encouraged to follow cybersecurity protocols that are based on recognized industry standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

i. Cybersecurity Threats

Updated security software/hardware should be installed, maintained, and updated regularly in order to protect against common cybersecurity threats. Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format.

a) Network systems must regularly test the security of IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.
b) 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.
c) All internal system violators should be subject to appropriate disciplinary actions for abuse.

ii. Access and Passwords

User access must be restricted based on job description or assigned duties. Authorized access must be reviewed on a regular basis to ensure access to sensitive systems is based on job requirements.

a) Computer and network access must be removed upon employee separation. Individuals with access to Information Technology (IT) systems must use individually assigned accounts.
b) 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. Processes that use more than one measure are preferred. These are referred to as two-factor authentication (2FA) or multi-factor authentication (MFA).
c) Passwords and/or passphrases must be changed as soon as possible if there is evidence of compromise or reasonable suspicion of a compromise exists.
d) Companies that allow their users to remotely connect to a network must employ secure technologies, such as virtual private networks (VPNs), to allow employees to access the company's intranet securely when located outside of the office. Companies must also have procedures designed to prevent remote access from unauthorized users.
e) If companies allow employees to use personal devices to conduct company work, all such devices must adhere to the company's cybersecurity policies and procedures to include regular security updates and a method to securely access the company's network.

8. 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. The following procedures must be included:

i. Access Controls and Personnel

a) Procedures for the issuance, removal and changing of access devices
b) Procedures to identify and challenge unauthorized or unidentified persons
c) Procedures to remove identification, facility, and system access for terminated employees.

ii. Incident Reporting

a) Procedures for employees to report security incidents and/or suspicious behavior, including the ability to do so anonymously

iii. Cargo Security

a) Procedures for the inspection of ocean containers or truck trailers prior to stuffing
b) Procedures to secure cargo staging areas including protection from unauthorized access and prevention of pest contamination as well as inspection for visible pest contamination on a regular basis
c) Procedures to control, manage and record the issuance and use of high security bolt seals for ocean containers and truck trailers. Such procedures must stipulate how seals are to be controlled and affixed to loaded containers and shall include procedures for recognizing and reporting compromised seals or containers to US Customs or the appropriate foreign authority and Boeing at supplychainsecurity@boeing.com.
d) Procedures for ensuring that information transmitted/received to/from service providers, subcontractors and agents, is reported accurately and timely
e) Procedures for ensuring 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

iv. Denied Party Screening

a) Procedures to identify any party on denied party lists maintained by the Department of Commerce/Bureau of Industry and Security (BIS), the Department of State/Directorate of Defense Trade Controls (DDTC), and the Department of Treasury/Office of Foreign Assets Control (OFAC)

v. Cybersecurity

Must have comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems.

a) 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.
b) Cybersecurity policies and procedures must be reviewed annually, or more frequently, as risk or circumstances dictate. Following the review, policies and procedures must be updated if necessary.
c) Cybersecurity policies and procedures should include measures to prevent the use of counterfeit or improperly licensed technological products.
d) Cybersecurity policies should address how a company shares information on cybersecurity threats with the government and other business partners.
e) Cybersecurity policies and procedures should include measures to prevent the use of counterfeit or improperly licensed technological products.
f) Companies that allow employees to use personal devices to conduct company work, must adhere to the company's cybersecurity policies and procedures to include regular security updates and a method to securely access the company's network.
g) All media, hardware, or other IT equipment that contains sensitive information regarding the import/export process must be accounted for through regular inventories. When disposed, they must be properly sanitized and/or destroyed in accordance with the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization or other appropriate industry guidelines.

9. Security Awareness Program

A Security Awareness 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 identifying and addressing unauthorized access,

proper ethical conduct, and avoidance of corruption, fraud and exploitation. Additional training on maintaining cargo integrity should be provided to employees in the shipping and receiving areas. Key personnel should receive regular training which shall be no less than once per year on security procedures and requirements.