Albany International Corp.
216 Airport Drive
Rochester, New Hampshire 03867 USA

Global Supply Chain Security Recommendations

These minimum security criteria are fundamentally designed to be the building blocks for foreign manufacturers to institute effective security practices designed to optimize supply chain performance 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 determination and scope of criminal elements targeting world commerce through internal conspiracies requires companies, and in particular, foreign manufacturers to elevate their security practices.

At a minimum, on a yearly basis, or as circumstances dictate such as during periods of heightened alert, security breach or incident, foreign manufacturers must conduct a comprehensive assessment of their international supply chains based upon the following C-TPAT security criteria. Where a foreign manufacturer out-sources 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 pertinent security measures are in place and are adhered to throughout their supply chain. The supply chain for C-TPAT purposes is defined from point of origin (manufacturer/supplier/vendor) through to point of distribution – and recognizes the diverse business models C-TPAT members employ.

C-TPAT recognizes the complexity of international supply chains and security practices, and endorses the application and implementation of security measures based upon risk[1]. Therefore, the program allows for flexibility and the customization of security plans based on the member's business model.

Appropriate security measures, as listed throughout this document, must be implemented and maintained throughout the Foreign manufacturer's supply chains - based on risk[2].

Business Partner Requirement

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

---

[1] *Foreign manufacturers shall have a documented and verifiable process for determining risk throughout their supply chains based on their business model (i.e., volume, country of origin, routing, C-TPAT membership, potential terrorist threat via open source information, having inadequate security, past security incidents, etc.).*

[2] *Foreign manufacturer shall have a documented and verifiable process for determining risk throughout their supply chains based on their business model (i.e., volume, country of origin, routing, potential terrorist threat via open source information, etc.)*

Security procedures
For those business partners eligible for C-TPAT certification (carriers, importers, ports, terminals, brokers, consolidators, etc.) the foreign manufacturer must have documentation (e.g., C-TPAT certificate, SVI number, etc.) indicating whether these business partners are or are not C-TPAT certified.

For those business partners not eligible for C-TPAT certification, the foreign manufacturer must require that their business partners to demonstrate that they are meeting C-TPAT security criteria via written/electronic confirmation (e.g., 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 C-TPAT security criteria or an equivalent World Customs Organization (WCO) accredited security program administered by a foreign customs authority; or, by providing a completed foreign manufacturer security questionnaire). Based upon a documented risk assessment process, non-C-TPAT eligible business partners must be subject to verification of compliance with C-TPAT security criteria by the foreign manufacturer.

Point of Origin
Foreign manufacturers must ensure that business partners develop security processes and procedures consistent with the C-TPAT 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.

Participation/Certification in a Foreign Customs Administration Supply Chain Security Program
Current or prospective business partners who have obtained a certification in a supply chain security program being administered by foreign Customs Administration should be required to indicate their status of participation to the foreign manufacturer.

Security Procedures
On U.S. bound shipments, foreign manufacturers should monitor that C-TPAT carriers that subcontract transportation services to other carriers use other C-TPAT approved carriers, or non-C-TPAT carriers that are meeting the C-TPAT security criteria as outlined in the business partner requirements.

As the foreign manufacturer is responsible for loading trailers and containers, they should work with the carrier to provide reassurance that there are effective security procedures and controls implemented 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 the container 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 ten-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
- Right side
- Floor
- Ceiling/Roof
- Inside/outside doors
- Outside/Undercarriage

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 C-TPAT. 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 controlled 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 (e.g. 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 unauthorized/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 timely.

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 C-TPAT 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.

Information Technology Security
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 provided to employees in the form of training.

Accountability
A system must be in place to identify the abuse of IT including improper access, tampering or the

altering of business data. All system violators must be subject to appropriate disciplinary actions for abuse.

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.

Albany International Corp.
216 Airport Drive
Rochester, New Hampshire 03867 USA

Global Supply Chain Security Acknowledgement and Survey

Note to Suppliers: Please only complete the survey if specifically instructed by Albany International Corp.

A	General Business Information			Description / Comments
1	Company Name:			
2	Address:			
3	Name, Title of Person Completing this Questionnaire:			
4	Expected number of international shipments from your facility to Albany International Corp.U.S. per month, over the next 12 months:			
5	General description of items shipped to Albany International Corp..:			
B	**Supply Chain Security Programs**	**Yes**	**No**	**Description / Comments**
1	Is your company (or your U.S. parent company or subsidiary) a C-TPAT member? If so, please provide the Status Verification Identification (SVI) number in the Comments section.			
2	Is your company a member of AEO or another WCO accredited security program administered by a foreign customs authority? If so, please indicate which program and provide documented proof of status.			
NOTE: If you answered "YES" to either of the above questions (confirming your company's status in C-TPAT, AEO, or similar supply chain security program), you do not need to complete the remainder of this survey.				
3	Is there a department that is responsible for supply chain security? If so, please name the department in the Comments section.			
4	Is there an employee with responsibility for supply chain security issues? If so, please provide the name and contact information (phone, email) in the Comments section.			
5	Do you conduct risk assessments of your supply chain? If so, please indicate the frequency in the Comments section.			

6	Do you resolve issues identified during the risk assessment?			
7	Do you have written requirements for logistics service providers (freight forwarders, trucking companies, brokers, etc.)?			
8	Do you require logistics service providers to have supply chain security measures in place? If yes, please describe in the Comments section.			
C	**Shipping/Conveyance Security**	**Yes**	**No**	**Description / Comments**
1	Do you have procedures in place at your container stuffing location to verify the physical integrity of the container (including the locking mechanisms on the doors) prior to stuffing?			
2	Do you conduct a 7-point inspection of all containers, prior to stuffing, to ensure the integrity of the: 1. Front wall 2. Left side 3. Right side 4. Floor 5. Ceiling and roof 6. Inside and outside doors 7. Outside and undercarriage			
3	Do you have a procedure for notifying the appropriate authorities if any illegal or suspicious activities are detected?			
4	Are containers and trailers stored in a secure area to prevent unauthorized access or manipulation?			
5	Is there a procedure for challenging and reporting unauthorized entry into the containers or the container storage area?			
6	Do you affix a high security seal to every loaded trailer and container bound for the United States?			
7	Do you use seals that meet or exceed the current PAS ISO 17712 standards for high security seals?			
8	Do you control which employees have access to (and distribute) the container seals?			
9	Do you have written procedures that describe how the seals are controlled during transit? If yes, do the procedures include:			

	a) Ensuring that seals are affixed to loaded containers during transit?			
	b) Verifying whether seals are intact or exhibit evidence of tampering during transit?			
	c) Reporting any compromised/damaged seal to the appropriate authorities?			
	d) Placing a second seal on a trailer and documenting the change if the first sea l was removed (even by a government official) while en route to the port of export?			
	e) Properly documenting the original seal and second seal (if the seal has been replaced during transit)?			
	f) Verifying that the seal number and location are the same as stated in the shipping documents?			
10	For international shipments bound for the United States, do you have procedures in place that require your trucking companies to track/monitor your shipments in transit and notify their dispatcher of any delays due to weather, traffic, or rerouting?			
11	Do you have specific procedures or training programs in place to prevent the hijacking of your outbound trailers?			
D	**Procedural Security**	**Yes**	**No**	**Description / Comments**
1	Do you have procedures to ensure that all information and documentation used in cargo clearance is legible, complete, and accurate?			
2	Do you have procedures for verifying the departing cargo against purchase orders or delivery orders, to ensure the correct items and quantities are being shipped?			
E	**Physical Access Control**	**Yes**	**No**	**Description / Comments**
1	<u>Employee Access:</u> a) Are employees required to show an identification badge when entering your premises?			
	b) Do employees use an electronic card reader to gain access?			
	c) Are employees only given access to the secure areas needed to perform their duties?			

	d) Are employee vehicles subject to search or inspection when entering or leaving the premises?			
2	Contractor Access: a) Are contractors required to show an identification badge when entering your premises?			
	b) Do contractors use an electronic card reader to gain access?			
	c) Are contractors only given access to the secure areas needed to perform their duties?			
	d) Are contractor vehicles subject to search or inspection when entering or leaving the premises?			
3	Visitor Access: a) Are visitors required to show photo identification upon arrival?			
	b) Are visitors required to display a temporary identification badge?			
	c) Are visitors required to be escorted by a company employee at all times?			
	d) Are visitor vehicles subject to search or inspection when entering or leaving the premises?			
4	Deliveries (including mail): a) Are delivery personnel required to show photo identification upon arrival?			
	b) Are arriving mail and packages periodically screened before being delivered to the recipient?			
5	Security Guards: a) Do you have security guards at the facility?			
	b) Are security guards on duty all day, every day (24 hours per day, 7 days per week)?			
	c) Are the security guards employees of the company?			
6	Do you have a procedure for identifying, challenging, and addressing/removing any unauthorized or unidentified people from your premises?			
F	**Physical Security**	**Yes**	**No**	**Description / Comments**

1	Are there fences enclosing your cargo handling and storage facilities?			
2	Do you have separate fenced areas that separate your domestic, international, high-value, and dangerous/hazardous cargo?			
3	If you have fences, are they regularly inspected for integrity and damage?			
4	Are there gates and gate houses that control the entry of vehicles and personnel to your premises?			
5	Are employee and visitor parking areas separated from the cargo handling and storage areas?			
6	Are your buildings constructed of materials that can resist unlawful entry, and are they maintained through periodic inspection and repair?			
7	Are all external and internal windows, gates, and fences secured with locking devices?			
8	Is the issuance of locks and keys controlled by management or security personnel?			
9	Is adequate lighting provided inside and outside the facility, in the following areas: a) Entrances and exits?			
	b) Cargo handling areas?			
	c) Storage areas?			
	d) Fence lines?			
	e) Parking areas?			
10	Do you have alarm systems and/or video surveillance cameras to monitor the premises and prevent unauthorized access to cargo handling and storage areas?			
G	**Personnel Security**	**Yes**	**No**	**Description / Comments**
1	Do you verify application information, such as employment history and references, prior to employment?			
2	If allowed by your local regulations, do you conduct background checks for prospective employees?			
3	Do you have procedures for removing identification badges, facility access, and computer system access for terminated/retired employees?			

H	Information Technology Security	Yes	No	Description / Comments
1	Do your computer systems require individual user accounts and passwords to gain access?			
2	Do your computer systems require employees to change their passwords on a periodic basis?			
3	Do you monitor your systems to identify abuse, improper access, and/or unauthorized alteration of business data?			
I	**Training and Awareness**	**Yes**	**No**	**Description / Comments**
1	Do you have a security training program to increase employee awareness of the potential terrorist threat to your supply chain?			
2	Are employees made aware of how to address and report a potential supply chain security issue?			
3	Do employees in your shipping/ receiving department and mail room receive additional training regarding cargo security?			
4	Do employees receive any special recognition or awards for identifying or reporting issues?			

_____(INSERT COMPANY NAME)_____acknowledges Albany International Corp.'s emphasis on global supply chain security and recognizes the expectation that business partners share that commitment. I understand that Albany International Corp. may refer security inquiries from U. S. Customs to the Supplier.

NAME: _____ TITLE_____

SIGNATURE: _____ DATE _____