Customs Trade Partnership Against Terrorism Security Requirements for Import Suppliers

To Our Import Suppliers:

CVS Pharmacy is committed to ensuring supply chain security within a framework consistent with Customs Trade Partnership Against Terrorism (CTPAT) guidelines and in a prudent, equitable and vigilant manner. The information included herein provides guidance regarding security criteria necessary to help safeguard our supply chain. These Minimum Security Criteria are designed for foreign manufacturers to institute effective security practices, to mitigate the risk of loss, theft and contraband smuggling that could potentially introduce terrorists and implements of terrorism into the global supply chain.

U.S. Customs and Border Protection (CBP) is asking businesses to ensure the integrity of their security practices and communicate their security guidelines to their business partners within the supply chain. In order to align our security program with CBP, CTPAT and industry standards, we request that you also align your factory security program accordingly as stated in the enclosed document. Our CTPAT Security Requirements for Import Suppliers must be shared with all non–U.S. based factories producing finished goods for CVS Pharmacy, including relevant business partners such as trucking and subcontracting facilities.

Please sign the “Agreement to Strengthen Supply Chain Security Consistent with CTPAT Guidelines”, located on page 12 of this document, and return within **7 business days**. If you should have any questions, please contact Cheryl Martin, Director, Customs Compliance, at Cheryl.Martin@CVSHealth.com or +1-401-770-6265. More information on CTPAT Security Criteria for Foreign Manufacturers can be found at CBP.gov/Border-Security/Ports-Entry/Cargo-Security/CTPAT.

Sincerely,

William May
Vice President of Transportation

CVS Pharmacy CTPAT Security Audit Program

Overview

To verify CTPAT compliance at the point of origin within the CVS Pharmacy supply chain, all manufacturing facilities, including subcontracting facilities that produce finished goods where CVS Pharmacy is the Importer of Record (i.e., the direct importer), are subject to onsite security audits. It is a CVS Pharmacy expectation that all supplier factories that fit within these criteria ensure they continually meet the **CVS Pharmacy CTPAT Security Requirements for Import Suppliers** (pp. 4–11). Ensuring that supplier factories consistently adhere to all of the CTPAT Minimum Security Criteria presented throughout this document can reduce the frequency of security audits and the need for corrective action, thus reducing additional expenses for the supplier factory. Language regarding CTPAT and our expectations has been added to the terms and conditions of our import purchase order. A copy of our purchase order terms and conditions can be found at CVSSuppliers.com.

Supplier Factory Business Partner Responsibilities

Supplier factories are also responsible for ensuring that any of their subcontracting facilities that produce finished goods for CVS Pharmacy are in full compliance with the **CVS Pharmacy CTPAT Security Requirements for Import Suppliers**. Additionally, supplier factories must also provide **Over-the-Road CTPAT Guidelines** (pp. 10–11) to all truck drivers responsible for transporting CVS Pharmacy cargo.

Third-Party Audit Service Provider

UL's Responsible Sourcing group, a division of Underwriters Laboratories LLC ("UL"), is the exclusive third-party audit provider for the CVS Pharmacy CTPAT Security Audit program. CVS Pharmacy uses UL's **Facility Security Template (FaST)** to conduct security audits in accordance with CBP's CTPAT Minimum Security Criteria for Foreign Manufacturers and best practice recommendations. UL will contact the supplier on behalf of CVS Pharmacy to register factory-related information into its system and will also notify the supplier when its factory is selected for a FaST audit.

Preparing for a FaST Audit

The **CVS Pharmacy CTPAT Security Requirements for Import Suppliers** must be communicated to all appropriate personnel who work in factories producing goods where CVS Pharmacy is the Importer of Record. Factories are responsible for creating and maintaining records of all procedures, logs, training and other applicable documentation relating to CTPAT security. Ensuring that supplier factories are in full compliance and are maintaining documentation for all of CBP's CTPAT Security Criteria for Foreign Manufacturers will increase the likelihood of a successful FaST audit.

FaST Audit Remediation

Factories with audit results that do not meet the CVS Pharmacy CTPAT security standards may be subject to a Corrective Action / Preventative Action (CAPA) plan at the supplier's expense. The purpose of the CAPA is to assist factories in correcting any CTPAT security deficiencies. Suppliers are required to partner with their factories during the CAPA process to ensure all requirements are met.

Forced Labor / Countering America's Adversaries Through Sanctions Act

In August 2017, U.S. President Trump signed into law a bill that imposed sanctions against North Korea (D.P.R.K.). Under the new law, there is now a presumption that any goods, wares, merchandise and articles made by North Korean citizens or nationals anywhere in the world should be considered goods made by forced labor. As a result, CBP is authorized to seize any shipment destined to the United States that is believed to have been made with forced and/or prison labor.

All suppliers and factories that produce goods for CVS Pharmacy are responsible for ensuring their factories do not employ North Korean citizens or nationals. The presence of North Korean labor will therefore be considered a Zero Tolerance finding for both Social Compliance and CTPAT Security audits. See CBP.gov/Trade/Programs-Administration/Forced-Labor for more information on forced labor.

CVS Pharmacy CTPAT Security Requirements for Import Suppliers

Business Partner Requirements

Foreign manufacturers must have written and verifiable processes for the selection of business partners, including truckers, subcontracting facilities and import product suppliers (e.g., parts and raw material suppliers), and they must develop and implement a sound plan to enhance security procedures.

Minimum Requirements:

- Signed and dated documentation of having communicated the CVS Pharmacy CTPAT Security Requirements for Import Suppliers to relevant business partners of the factory.
  - **NOTE:** Business partners include subcontracted manufacturing facilities producing finished goods for CVS Pharmacy (if applicable) and truckers responsible for transporting the cargo.
- Maintain an active list of the factory's business partners **eligible** for CTPAT, indicating whether or not the business partners are **active members** of CTPAT.
  - **NOTE:** Please visit CBP.gov/Border-Security/Ports-Entry/Cargo-Security/CTPAT for more information on CTPAT eligibility.
- Business partners of the factory **not** eligible for CTPAT must be required to demonstrate in writing that they are complying with CTPAT Minimum Security Criteria.
- Based on risk, reviews of the business partners' processes and facilities should be conducted on a periodic basis via site visits, a questionnaire or similar means.

Cybersecurity

Cybersecurity is the key to safeguarding intellectual property, customer information, financial data and employee records, among other assets. Facilities must have comprehensive written cybersecurity policies and/or procedures to protect information technology systems.

Minimum Requirements:

- Have a written cybersecurity policy and/or procedures to protect information technology.
- Install sufficient software/hardware protection from malware (e.g., viruses, spyware).
- Ensure security software is current and receives regular updates.
- Have a business resumption plan in place that addresses how to retrieve data in the event of a catastrophic event or emergency.

- Regularly test and document the security of the IT infrastructure; if vulnerabilities are found, corrective action must be implemented and documented.
- Individuals with access to Information Technology systems must have individually assigned accounts.
- Procedures must state that system passwords must be changed at a minimum every **90 days**.
- Access to company technology must be limited to the job responsibilities of each employee.
- Procedures must address how both to identify and discipline employees for the abuse of technology, including improper access, tampering and altering of business data.
- Cybersecurity policies and procedures should include measures to prevent the use of counterfeit or improperly licensed technological products.
- Procedures must state that system data must be backed up on a regular basis. CBP has recommended as a best practice that system data should be backed up daily.
- Facility must take regular inventory of all media, hardware or other IT equipment.

Container Security

Procedures must be in place to verify the physical integrity of the container and/or truck structure prior to stuffing, to include the reliability of the locking mechanisms used on the doors.

Minimum Requirements:

- A Seven-Point Inspection (see **Exhibit A**) must be conducted prior to loading all containers, including: Front Wall, Left Side, Right Side, Floor, Ceiling/Roof, Inside/Outside Doors, Outside/Undercarriage.
  - **NOTE:** Seven-Point Inspection records for each container must be maintained for at least **90 days**. CBP has recommended as a best practice to maintain these records for at least 12 months.
- Container inspection must include inspection of doors, handles, rods, hasps, rivets, brackets and all other parts of a container's locking mechanism for tampering or hardware inconsistencies.
  - **NOTE:** This inspection must be documented and maintained for at least **90 days**.
- Containers 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 or container storage areas.
- An ISO 17712 high-security bolt seal must be used on all containers bound for the U.S. (see **Exhibit B**).
  - **NOTE:** For full-container-load (FCL) CVS Pharmacy shipments, an ISO 17712 high security seal will be provided by the ocean carrier.

- Written procedures must stipulate how seals are controlled and affixed to loaded containers, including procedures for how to recognize and report compromised seals and containers. Additionally, these procedures must include the **VVTT** process:
  - **V:** *View* the seal and container locking devices to ensure no physical damage.
  - **V:** *Verify* that the seal number matches the shipping documentation.
  - **T:** *Tug* on the seal to ensure it is affixed properly.
  - **T:** *Twist* and turn the seal to ensure it does not unscrew.
- Only designated employees (preferably management) should be allowed to distribute container seals for integrity purposes.
- Seals must be stored in a designated and locked area (e.g., drawer or cabinet) during the loading process or anytime they are not in use. This storage area should be clearly marked as “Seals Only”.
- All seals and container numbers should be recorded and maintained in a log for at least **90 days**. CBP has recommended as a best practice to maintain seal and container numbers for at least 12 months.
- Less-than-container-load (LCL) shipments bound for the CVS Pharmacy Container Freight Station / Consolidator must have an adequate temporary seal or lock affixed to the truck/trailer to secure the cargo while in transit.
- Written procedures must be in place that outline what to do if a credible (or detected) threat to the security of a shipment or container is discovered. The facility must alert any business partners that may be affected and any law enforcement agencies, as appropriate.
- An outbound shipment log (**Exhibit C**) must be used to record details of all shipments departing the facility. Outbound shipment logs should be maintained for at least **90 days**.

Procedural Security

Protocols for the handling of incoming and outgoing goods must include protection against the introduction, exchange or loss of any legal or illegal material. It is recommended that procedures be written to help maintain a uniform process over time.

Minimum Requirements:

- A documented security policy should be in place that includes all elements of the CTPAT Minimum Security Criteria for Foreign Manufacturers (refer to CBP.gov/Border-Security/Ports-Entry/Cargo-Security/CTPAT).
- All incoming commercial vehicles, including the driver, must be identified, confirmed for valid purpose upon entry and documented in a driver log.
- Only security officers or designated personnel, not responsible for loading, should be allowed to inspect the container during both the loading and unloading processes.
- Written work instructions for security guards should be part of the factory policy.
- All cartons must be properly marked, weighed and counted.
- Documented written procedures must be in place for:

- Verifying seals on containers, trailers and railcars.
  - **NOTE:** Seal numbers should be electronically printed on the bill of lading.
- Verifying, detecting and reporting both overages and shortages.
- Tracking the timely movement of incoming and outgoing goods.
- Proper storage of empty and full containers to prevent unauthorized access.
- Notifying both domestic and U.S. customs officials and/or other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected.

Agricultural/Pest Security for Conveyances

Written procedures designed to prevent visible pests and contaminants into the United States via all types of conveyances and cargo must be created. The introduction of foreign animal and plant contaminants such as soil, manure, seeds and plant and animal material which may harbor invasive and destructive pests and diseases must be controlled. The first step to prevent conveyance contamination is to inspect the exterior and interior of conveyances prior to loading. A pest inspection log should be maintained (see **Exhibit D**).

Minimum Requirements:

- Provide personnel with training to know how to detect pests and contaminants.
- Monitor the cargo staging area to ensure the area is free from plants and plant pests.
- Monitor inside building(s), outside building(s), in and around containers and container areas.
- A visual inspection of cargo and shipping containers (interior and exterior) must be performed to check for contaminants and pests before loading.
- Vacuum, sweep, blow out or (if necessary) wash containers prior to loading.
- Container pest inspection records for each container must be maintained for at least **90 days**, detailing who did the pest inspection as well as what was done to remove any visible pests or contaminants.

Physical Security

All buildings must be constructed of materials that resist unlawful entry and protect against outside intrusion.

Minimum Requirements:

- Fencing must fully enclose the perimeter of the facility, including the cargo handling and storage areas.
- Loading and packing areas must be secure enough to prevent unauthorized access.
  - Loading and packing areas should be inspected on a regular basis to ensure areas remain free of visible pest contamination.
- Entrance and exit gates to the facility must be manned and monitored.

- Facility must have working locking devices for all external and internal doors, windows, gates and fences.
- Facility must segregate and mark international, domestic, high-value and dangerous cargo within the warehouse by a safe, a cage or an otherwise fenced-in area.
- Adequate lighting must be provided in all of the following areas: entrances, exits, cargo handling, storage areas, fence lines and parking areas.
- Fully functioning alarm systems and video surveillance cameras should be used to monitor the facility, including but not limited to the cargo handling and storage areas.
  - There must be a written policy and procedure in place governing the use, maintenance and protection of the video surveillance and alarm system.
  - Periodic, random reviews of video surveillance footage should be conducted by management, security or other designated personnel to verify that cargo security procedures are being followed.
- A minimum of **30 days** of video surveillance should be maintained on record at all times. CBP has recommended as a best practice to maintain video surveillance for 90 days.
- Parking areas for private passenger vehicles must be separated from the shipping, loading dock and cargo areas. A communication system (e.g., intercom, walkie-talkies, telephone) must be in place to contact internal security personnel or local law enforcement.
- All facility keys and access codes must be controlled by management.
- Records of routine inspections for the facility must be maintained for at least **90 days**. CBP has recommended as a best practice to maintain these records for at least 12 months.
- Protocols must be in place to prevent any tampering of sealed cartons.

Access Controls

The positive identification of all employees, vendors and visitors (business clients including CVS Pharmacy employees, delivery drivers and so forth) is required. Unauthorized access to the shipping, loading dock and cargo areas must be prohibited.

Minimum Requirements:

- Photo identification badges for all employees and temporary workers must be worn visibly at all times while on the premises of the facility.
- All visitors must present photo identification upon arrival at the facility, and the following information must be recorded in a visitor log at a minimum:
  - Date
  - First and last name
  - Visitor signature
  - Verification of photo identification (type verified as license or national ID card)
  - Company
  - Time in and time out

- All visitors must have temporary badges visibly worn at all times while on the premises.
- All visitors must be escorted and monitored while on the premises.
- At least **6 months** of visitor log information must be maintained. CBP has recommended as a best practice to maintain visitor logs for at least 12 months.
- Employees must have access only to areas where they need to perform their job functions.
- An identification system must be in place that designates employees to specific areas of the facility (e.g., differently colored badges that signify who is allowed to be in certain areas of the facility).
- Written procedures must be in place to identify and authorize all persons entering the loading area.
- Written procedures for challenging unauthorized or unidentified individuals must be in place.
- Written procedures must be in place to remove identification and facility access immediately for terminated employees.
- Incoming mail and packages must be screened periodically to identify any suspicious substances or unusual activity (e.g., ticking noises), and procedures must be in place to educate employees on how to report suspicious packaging.
- Drivers delivering or receiving cargo must be identified before cargo is received or released.
- Facility must maintain in a secure manner a cargo pickup log that notates name, date and time of arrival, employer, truck/trailer number, departure time and seal number used at time of departure.

Personnel Security

Factories must have written policies on how to conduct employment screening and interviewing of prospective employees, to include periodic background checks and application verifications to the extent possible and allowed under local law.

Minimum Requirements:

- Employee applications that document past work history and references must be verified prior to employment.
- Official identification documents must be maintained on file in a secured area for all employees, including temporary workers.
- Consistent with local laws and regulations, background checks and investigations should be conducted for prospective employees and periodically for current employees based on cause and/or the sensitivity of the employee's position.
- Background checks should be verified for any contracted security personnel prior to hire.
- Procedures must be in place to remove identification, facility and system access for terminated employees.

- Facility must have an Employee Code of Conduct that includes expectations and defines acceptable behaviors. Employees and contractors must acknowledge receipt.

Training and Threat Awareness

A security training and threat awareness program must be in place to educate employees on the threats posed by terrorists and contraband smugglers. These programs must encourage active employee participation in recognizing and reporting internal conspiracies, including maintaining cargo integrity and procedures for challenging individuals who are prohibited from accessing specific areas of the facility.

Minimum Requirements:

- Threat awareness training should be provided to all employees at least **once per year**. Training records with the information below must be maintained for all active employees:
  - Date of training
  - Content overview
  - Facilitator name
  - Employee name and signature
  - Employee position
- Additional training pertaining to recognizing, investigating and/or reporting suspicious cargo should be provided to all security guards and employees working in packing, warehouse and shipping/receiving areas.
  - **NOTE:** Refer to the "Security and Threat Awareness Mindmap" at www.cbp.gov/sites/default/files/documents/Security%20Training%20and%20Threat%20Awareness%20Mindmap.pdf as a reference tool for developing CTPAT training content.
- As applicable based on position, employees must be trained on cybersecurity policies.

Over-the-Road CTPAT Guidelines

Factories must provide in writing security guidelines to all inland truckers transporting cargo for CVS Pharmacy. Factories also must maintain signed documentation from all truckers that they have received these guidelines.

Minimum Requirements:

- Procedures that stipulate how containers are subject to seal verification in the event the driver must leave the vehicle for any reason (e.g., during a rest stop) before arriving at the destination.
- Replacement seal procedures that address seal removal by government officials while containers are at the port or if a seal has been compromised while in transit.
- Reporting procedures for updating replacement seal numbers on all appropriate shipping documents before leaving the port of export.

- Factory should collaborate with their transportation provider to track conveyances from origin to final destination point.
- GPS tracking system should be used to monitor containerized cargo and to verify predetermined routes identified by management**.**

CVS Pharmacy Business Partner Agreement

Overview

CVS Pharmacy has implemented a procedure that requires each supplier to review and sign the attached **Agreement to Strengthen Supply Chain Security Consistent with CTPAT Guidelines**. This agreement states that the supplier will establish procedures consistent with the security recommendations posted on CBP.gov/Border-Security/Ports-Entry/Cargo-Security/CTPAT and will communicate the information to manufacturing business partners in a documented and verifiable format. A copy of the agreement is found on the next page.

Required Signatory

A company officer (i.e., the purchase order vendor of record) must sign the Agreement.

Submission

The Agreement on page 12 must be signed and emailed to David.Prata@CVSHealth.com within **7 business days**.

Consequence of Default

CVS Pharmacy reserves the right to use payment leverage methods if the agreement is not tendered in a timely manner. Questions regarding these procedures may be directed to Cheryl.Martin@CVSHealth.com.

Agreement to Strengthen Supply Chain Security
Consistent with Customs Trade Partnership Against Terrorism Guidelines

The Import Supplier agrees to develop and implement, within a framework consistent with the Customs Trade Partnership Against Terrorism (CTPAT) security criteria, a verifiable, documented program to enhance security procedures throughout its supply chain process, including, but not limited to, its manufacturing business partners. Where the Import Supplier does not exercise control of a production facility, transportation/ distribution entity or process in the supply chain, the Import Supplier agrees to communicate the CTPAT security criteria to its manufacturers and transportation/distribution service providers and, where practical, condition its relationships to those entities on the acceptance and implementation of the CTPAT security criteria.

The Import Supplier agrees to communicate the CVS Pharmacy supply chain security and CTPAT procedures to its manufacturers in a documented and verifiable format that can be made available upon request, and it understands that failure to do so may jeopardize its business relationship with CVS Pharmacy.

Supplier Name: _____

CVS Pharmacy Supplier #: _____

Supplier Address: _____

Signature (Company Officer): _____

Company Officer Title: _____ **Date:** _____

Domestic Representative Name: _____

Domestic Representative Telephone Number: _____

Domestic Representative Email: _____

Is your company a CTPAT member with U.S. Customs and Border Protection?

Yes | No

Is your company a member of a non-U.S. supply chain security program (e.g., AEO)?

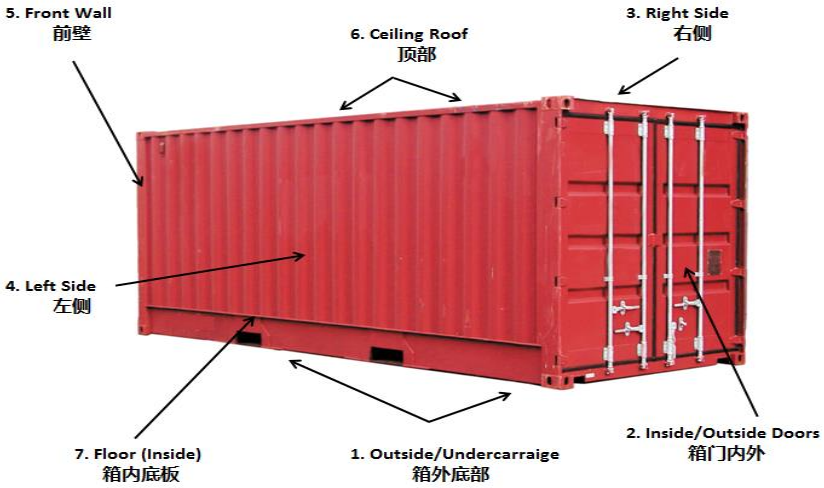
Yes | No

Some language in this agreement is derived from publications listed at CBP.gov/Border-Security/Ports-Entry/Cargo-Security/CTPAT.

Exhibit A

Seven-Point Container Inspection

Date of Inspection: _____



Please ☑ for Yes

1. Outside/Undercarriage	2. Inside/Outside Doors
□ Check for structural damage (e.g., dents, holes, repairs).	□ Ensure locks are secure and reliable.
□ Support beams are visible.	□ Check for loose bolts.
□ Ensure no foreign objects are mounted on container.	□ Ensure hinges are secure and reliable.
3. Right Side	**4. Left Side**
□ Look for unusual repairs to structural beams.	□ Look for unusual repairs to structural beams.
□ Repairs to the inside wall must be visible on the outside and vice versa.	□ Repairs to the inside wall must be visible on the outside and vice versa.
5. Front Wall	**6. Ceiling/Roof**
□ Front wall should be made of corrugated material.	□ Ensure beams are visible.
□ Interior blocks are visible and not false or absent. (Cardboard blocks are not normal.)	□ Ensure ventilation holes are visible. They should not be covered or absent.
□ Ensure vents are visible.	□ Ensure no foreign objects are mounted to the container.
7. Floor (Inside)	**8. Seal Verification**
□ Ensure floor of container is flat.	□ Seal properly affixed.
□ Ensure floor is uniform height.	□ Seal meets or exceeds PAS ISO 17712 standards.
□ Look for unusual repairs to the floor.	□ Ensure seal is not broken/damaged.

Before loading the container, you must conduct a seven-point inspection to ensure the safety of the whole container. If a container for CVS Pharmacy is damaged, or there is evidence of tampering, please contact Yusen Logistics for resolution prior to shipping.

Container Number: _____

Seal Number: _____

Full Name: _____

Signature: _____

Exhibit B

ISO 17712 High-Security Seal

Exhibit C

Example of a Factory Outbound Shipment Log

Factory Name:										
Factory Address:										
Factory Contact Phone Number:										
Carrier	**Driver Name**	**Container / Trailer Number**	**Seal Number (if applicable)**	**Destination**	**CVS Pharmacy Purchase Order**	**Item Number**	**Manifest Quantity**	**Date Loaded**	**Time Loaded**	**Security Guard Name**
Bill's Trucking	Bill Smith	ABCU1234567	123456	Port of Shanghai	1234567	123456	100	2019-12-31	13:00	Sam Jones

Exhibit D

Example of a Factory Agricultural/Pest Security Check Conveyance Log

Factory Name:					
Factory Address:					
Factory Contact Phone Number:					
Container Number	**Date of Inspection**	**Time of Inspection**	**Was container cleaned? Vacuumed, swept, or blown out?**	**Name and title of who inspected/cleaned the container**	**Destination**
ABCU1234567	2019-12-31	13:00	Swept	John Doe / Factory Manager	Port of Shanghai