Pep Boys Foreign Vendor CTPAT Security Manual –Requirements and Training Material

2017

Version 4.0

Updated October 2017

Dear Business Partner,

The Pep Boys – Manny, Moe, and Jack is a certified Tier III participant of the CTPAT program (Customs-Trade Partnership Against Terrorism) a partnership between the trade community and U.S. Customs and Border Protection (CBP) designed to establish supply chain security processes to prevent terrorist devices and other contraband from entering the global supply chain.

As a member of the CTPAT program, Pep Boys is required to engage with all of our business partners in order to aid you in developing and maintaining a security program within the guidelines of the CTPAT program, with emphasis on ensuring the integrity of all U.S. bound shipments. Together we will work to prevent the introduction of unauthorized materials into any cargo, container, trailer or other shipping conveyance.

This document is intended to ensure that all Pep Boys vendors, suppliers, and manufactures have access to the necessary training materials needed to be compliant with Pep Boys CTPAT program. The latest version of this document is available on our website at info.pepboys.com/ under Shipping Info – Import Requirements along with other import and CTPAT resources. After reviewing the criteria, you should implement any security and/or trade compliance improvements necessary to become compliant, and consider applying for CTPAT membership, if eligible.

If you are a member of the CTPAT program, please email your Status Verification Interface (SVI) number Martina_Gring@pepboys.com. In concert with U.S. CBP and the World Customs Organization, several other countries have developed similar, equivalent programs. These include Canada's Partners in Protection program (PIP), and what many other countries have designated as an Authorized Economic Operator program. If you are a member of one of these programs, please forward us a certificate of membership from your customs agency. For more information on these programs, please contact us or your own country's customs service.

If you are not a member of the CTPAT program, or an equivalent, we ask that you complete and return to us a "Foreign Vendor CTPAT Security Survey" on your current security procedures. Completion of this questionnaire will aid us in determining what assistance we can give towards enhancing your security program. Full and complete responses to this questionnaire will also aid us in determining how frequently we may be required under the CTPAT criteria to conduct site visits to verify security processes are in place.

It is also important that you educate all business partners you select on our behalf (suppliers, shippers, consolidators, trucking companies, and all other logistics partners) about the CTPAT program. Particular emphasis on trailer and container inspections, seal processes, live-time tracking and monitoring of cargo en route, personnel and access control security, and security awareness training is requested. Inspections of containers should be documented, and a copy of the completed inspection sheet (Page 11) forwarded

to The Pep Boys along with the other documents associated with the shipments through Agility our customs house broker and freight forwarder.

Please remind your partners that all loaded U.S. bound containers/trailers must be secured with an ISO 17712:2013 high security seal. You must also have written procedures within your supply chain for recognizing and reporting compromised seals on your containers and trailers to CBP or appropriate foreign authorities, and for challenging unknown or unauthorized persons within your facilities. If you should need assistance with any of these issues, please contact us for further information and training.

In sum, we are asking all our business partners to have a documented cargo and supply chain security program. Please contact us at the below phone numbers or email us with questions regarding CTPAT, developing your own security plan, or any other supply chain security matters.

Please refer to the following document for detailed information on the CTPAT program and for training materials to distribute to your employees. The document titled "Foreign Vendor CTPAT Security Survey" must be read carefully, completed fully and return to us.

Sincerely,
The Pep Boys - Manny, Moe & Jack

Martina Gring
Logistics Specialist
The Pep Boys - Manny, Moe & Jack
3111 West Allegheny Ave.
Philadelphia, PA 19132
Phone: 215-430-9430
Email: Martina_Gring@Pepboys.com

George Pavlichko
Director of Global Logistics
The Pep Boys - Manny, Moe & Jack
3111 West Allegheny Ave.
Philadelphia, PA 19132
Phone: 215-430-9059
Email: George_Pavlichko@Pepboys.com

CTPAT MINIMUM SECURITY REQUIREMENTS

Physical Security

1. Cargo handling and storage facilities must have physical barriers and deterrents that guard against unauthorized access.
2. Your facility must have a fence that secures the entire perimeter including the shipping and receiving area. The fence should also be locked when not in use and monitored by a guard house. We suggest that barbed wire or another trespassing deterrent is also in place.
3. Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored.
4. Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas.
5. Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.
6. 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.
7. 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.
8. Alarm systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas.
9. Testing of security systems (alarms, cameras, etc.) and procedures should be preformed periodically.

Physical Access Controls

1. An employee identification system must be in place for positive identification and access control purposes.
2. Employees should be issued ID badges and must be identified by a guard upon entrance to the facility.
3. All visitors must be identified via valid ID, given Visitor Badges, added to a Visitors Log (example below), and escorted for the duration of their visit.
4. Delivery persons must be positively identified via valid ID and their packages inspected.
5. Drivers must be positively identified when picking up the containers for delivery.
6. A documented process should be in place to identify and remove unauthorized/unidentified persons from the premises. All employees must be trained in this process.

Example Visitor's Log

Last Name	First Name	ID# (provided by visitor)	Purpose	Date	Time In	Time Out	Badge #
Smith	John	555 555 555	Job Interview	1/10/2016	9:05 AM	10:30 AM	1

Personnel Security

1. Prospective employees must be subject to background and reference checks.
2. A procedure should be in place to debrief terminated employees and collect all company property that they may have including ID badges. Computer access should be revoked. Security should be alerted that the person no longer has access.

Procedural Security

1. All shipping documents (Bills of Lading, Packing List, Commercial Invoice, and Container Manifest) must be audited or reviewed for correctness.
2. This process aims to identify shortages, overages, or other significant cargo discrepancies.
3. Any discrepancies identified must be investigated and resolved.
4. Employees must be trained on auditing procedures to ensure that all shipping documents are complete and accurate
5. All documents must be completed, audited, and forwarded to Agility 24 hours prior to delivery of the container to the pier.
6. Cargo descriptions including weight, pieces, and marks must be verified prior to loading the container.

Information Technology Security

1. Passwords should be required to log into company databases and computer systems.
2. A firewall should be installed to protect the company's computer system.
3. A system must be in place to identify the abuse of IT including improper access, tampering or the altering of business data.
4. Automated systems must use individually assigned accounts that require a periodic change of password.
5. Databases must be accessible by unique log in ID and password for each employee.
6. Password should expire every 30-60 days and be monitored by the IT department.

Security Training and Threat Awareness

1. Procedures should be in place in the event security is compromised.
2. Employees should be properly trained to follow all security procedures.
3. All security procedures should be documents and all employees must have knowledge of and access to this documentation.
4. Training on security procedures, seal and container inspection, unauthorized entry, and IT security should be given to all employees on a yearly basis.
5. Specific training should be given to employees based on their position on handling seals, completing and auditing shipping documents and the 7-point container inspection process.
6. Specific training should be offered to assist employees in maintaining cargo integrity, recognizing internal conspiracies, and protecting access controls.

Business Partner Requirements

1. Factories must have written and verifiable processes for the selection of business partners and sub-contractors.
2. Internal requirements, such as financial soundness, capability of meeting contractual security requirements, and the ability to identify and correct security deficiencies as needed, should be addressed.
3. Periodic reviews of business partners' processes and facilities should be conducted based on risk.

Container Security

1. Container integrity must be maintained to protect against the introduction of unauthorized material and/or persons.
2. Procedures must be in place to properly inspect, seal, and maintain the integrity of all shipping containers.
3. A high security seal must be affixed to all loaded containers bound for the U.S. All seals must meet or exceed the current ISO 17712:2013 standards for high security seals.
4. Procedures must be in place to verify the physical integrity of the container structure prior to stuffing, including examining the reliability of the locking mechanisms on the doors.
5. Written procedures must stipulate how seals are to be controlled (distributed) and affixed to loaded containers. See pages 7-9.
6. A seven-point inspection process is required for all containers. See pages 10-15.
7. Procedures should include directions for recognizing and reporting compromised seals and/or containers to US Customs and Border Protection or the appropriate foreign authority.
8. Only designated employees should distribute container seals for integrity purposes.
9. Containers must be stored in a secure area to prevent unauthorized access and/or manipulation.
10. Procedures must be in place for reporting and neutralizing unauthorized entry into containers or container storage areas.
11. Prior to stuffing all export bound containers must be stored in a gated yard within your facility.
12. A packing list must be attached to the inside of the container door or to the last pallet/box loaded into the container.

Import Vendor Container Stuffing Requirements

1. All containers must be booked through our nominated Freight Forwarder and Customs House Broker Agility-Geo Logistics.
2. The container must be drayed to your secured facility as advised on your 10+2 Information Request Form.

3. Once the container has been assessed per the 7-point container inspection sheet (page 11), the merchandise maybe loaded.
4. Vendors are required to submit a container load plan and 7-point container inspection sheet with their commercial documents to Agility prior to delivery of the container to the pier.

Seal Requirements

Please be advised that effective **May 15 2014,** the former International Organization for Standardization (ISO) mechanical seal standard (ISO 17712:2010) will be replaced with a new ISO standard—ISO 17712:2013. CTPAT understands that seals are costly, and companies are not expected to discard seals currently in stock. However, after companies have exhausted their current stock of high security seals, we recommend that they purchase seals which are compliant with the new ISO 17712:2013.

The new standard compliance requirements:

1. Testing to determine a seal's classification for physical strength (as a barrier of entry).

   ISO 17712 defines three types of classes of seal strength or barrier capacity: "I" for Indicative; "S" for Security; and "H" for High Security. **CTPAT requires the use of "H" class seals.** Suppliers must use independent third party test laboratories to validate a seal's classification. Labs must be accredited per ISO/IEC 17025 (General requirements for the competence of testing and calibration laboratories) to perform testing specific to ISO 17712.

2. Process for auditing of the manufacturer's security-related business practices.

   Poor security-related practices can undercut the effectiveness of a high-quality security seal. ISO 17712's Annex A defines over two dozen required practices, such as facility risk assessments and access controls to production and storage areas. Suppliers' conformance with Annex A should also be demonstrated through an independent certification provider that is accredited to audit compliance with the ISO standards.

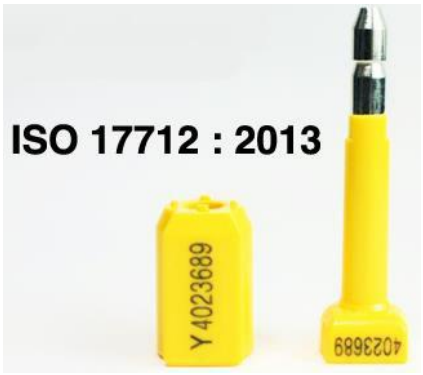
3. Seals be designed and constructed with tamper indicative features that generate tell-tale evidence of tampering.

   Seal manufacturers must be able to demonstrate to, and obtain certification from, an accredited auditor from an independent third party organization that their high security seals have built-in tamper evidence features. If an independent third party organization accredited to ISO 17020 verifies conformity, it will provide the manufacturer with a certificate of compliance that documents that the seals submitted for review do reflect tell-tale evidence of tampering generated by attempts to defeat a correctly closed and affixed seal.

Considering that most seals are tampered with in order to introduce illegal contraband or to pilferage a container, this is a welcomed improvement for high security seals –particularly those that are U.S. bound and those affixed to CTPAT containers and trailers.

Benefits of the new seal standards include:

1. Reduced possibility of cargo theft or tampering
2. Reduced possibility of unauthorized material being inserted into containers or other instruments of international traffic (IIT).
3. Reducing shipping delays that result when seals are missing or broken.
4. When inspecting seals for signs of tampering, tamper-evident seals should allow personnel, with the appropriate training, to detect compromised seals easier.

Example: 

Partners are reminded to be vigilant in their purchase of ISO 17712 compliant seals.

1. They should be obtaining independent written certification from a supplier that its product and processes meet or exceed the ISO 17712 standard. Partners should ask their suppliers for copies of conformance certificates for product testing and security related business practices (Normative Annex A).

2. The certificates for product testing should come from a lab that is properly accredited according to ISO procedures, such as ISO 17025. The test house must be accredited by an independent third party test laboratory.

Beware of fraudulent documents. Some independent laboratories have adopted digitally signed and certified test reports to ensure content integrity and author authenticity.

Seal Use Monitoring

To maintain the integrity of the cargo stored for transport we require that you do the following regarding the storage and integrity of Export Container Seals.

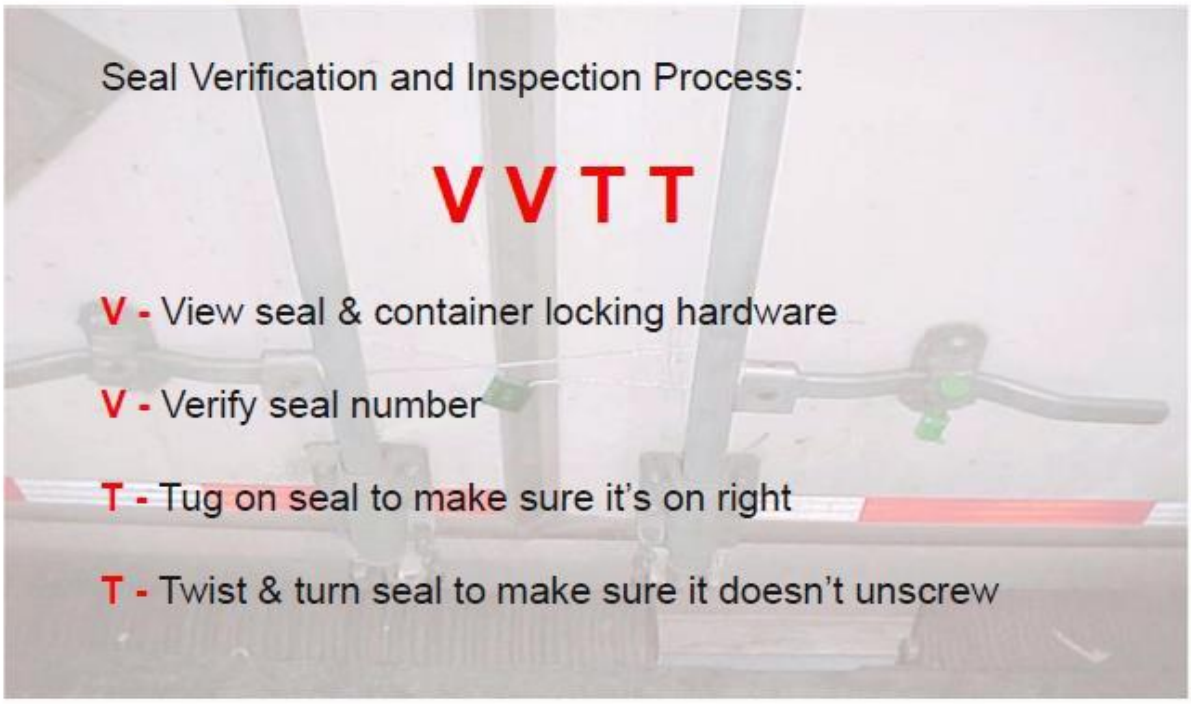
1. A Seal Inventory Log must be kept to monitor seal usage. It should include the date and container the seal was affixed.

Example Seal Log

Date	Seal	Container	PO	Customer
2/20/2016	AR050012	TEMU2726410	A01345	Pep Boys

2. Seals must be kept in a locked and secure location prior to their use.
3. Only authorized personnel should have access to seals. The fewer people who have access to seals, the better.
4. Unauthorized employees must never handle seals.
5. Seals should be affixed to the right door of the container/ trailer on the hasp that has the welded rivet. This practice will raise the level of security for the shipment.
6. After the seal is affixed to the container, an authorized employee should make sure that the seal is secure by pulling down on it.
7. Seals will be inspected upon delivery to Pep Boys for evidence of tampering and the seal number verified.

Seal Inspection

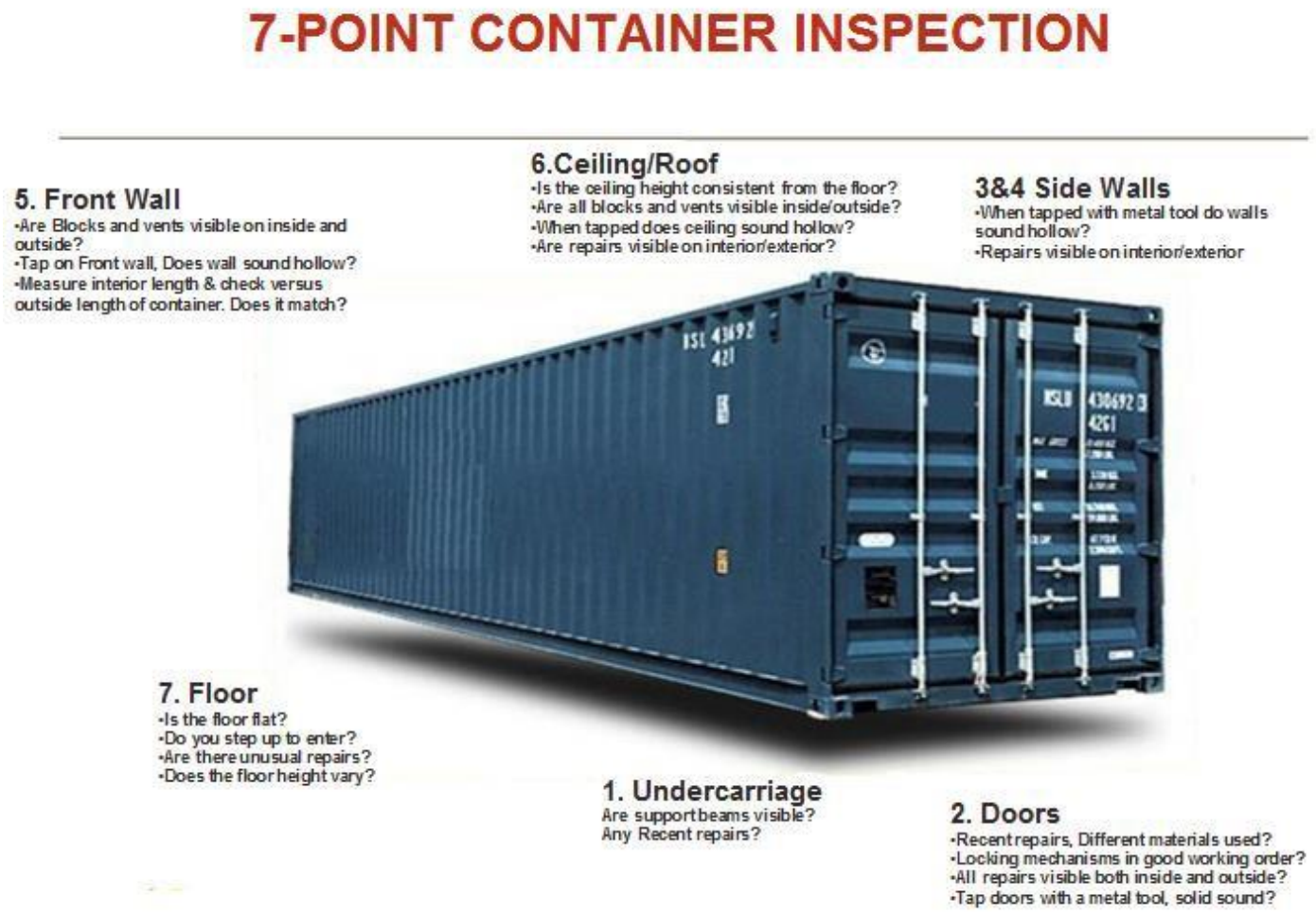


Required 7 Point Container Inspection

To fortify the security of our supply chain we must monitor the physical integrity of all containers and trailers delivered for export to Pep Boys.

All containers are subject to the following 7-point inspection upon delivery.

1. **Outside/ Undercarriage**
2. **Inside/Outside Doors**
3. **Left Side Wall**
4. **Right Side Wall**
5. **Front Wall**
6. **Ceiling/Roof**
7. **Floor**



The following sheet (page 11) must be completed upon loading the container and delivered with the commercial documents to Agility Logistics. Each container must have a completed 7-point container inspection sheet.

7 Point Container/Trailer Physical Integrity Delivery Sheet

Inspector _____
Title or Position _____
Factory Name _____
Date and Time _____
Container/Trailer No _____
Seal No _____
PO No _____
Carrier _____

Please check the appropriate box regarding the condition of the container or trailer. If yes is selected, please describe the damage below.

	Damage Assessment	
Container Inspection	**Yes**	**No**
Front Wall		
Left Side		
Right Side		
Floor		
Ceiling/Roof		
Inside/Outside Doors		
Outside/Undercarriage		

Seal Number Accurate: Circle**: Yes / No**
Seal Condition: Circle**: Approved / Tampered**

_____

_____

_____

I have inspected the above listed container/trailer.
Signature _____ **Date** _____

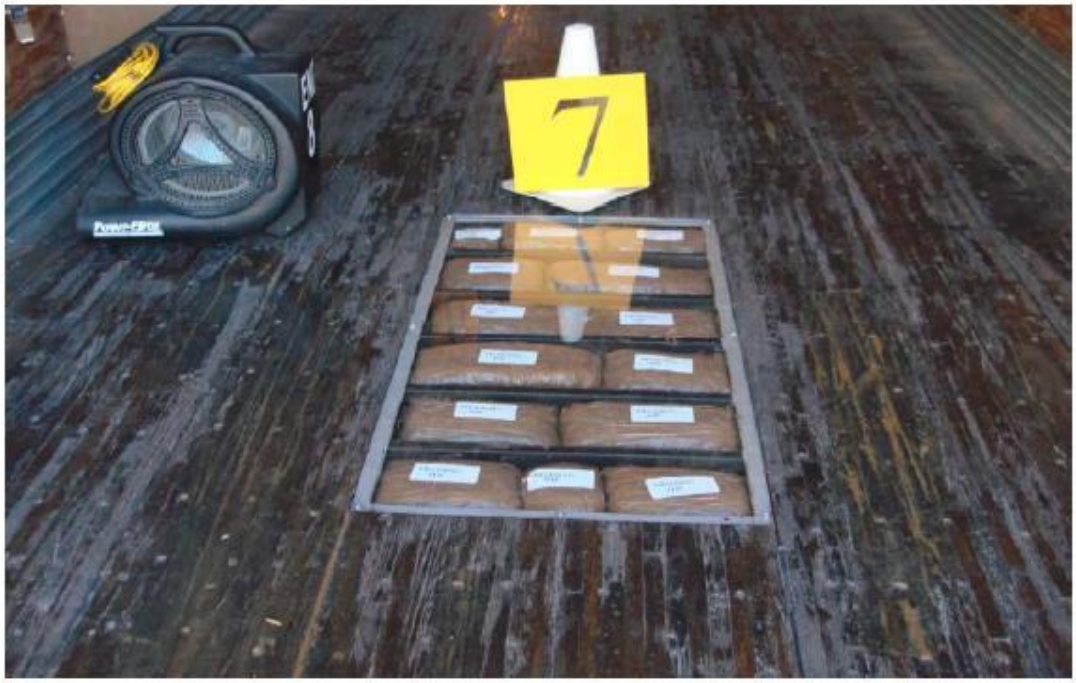
We're car people.

Evidence is Always Present

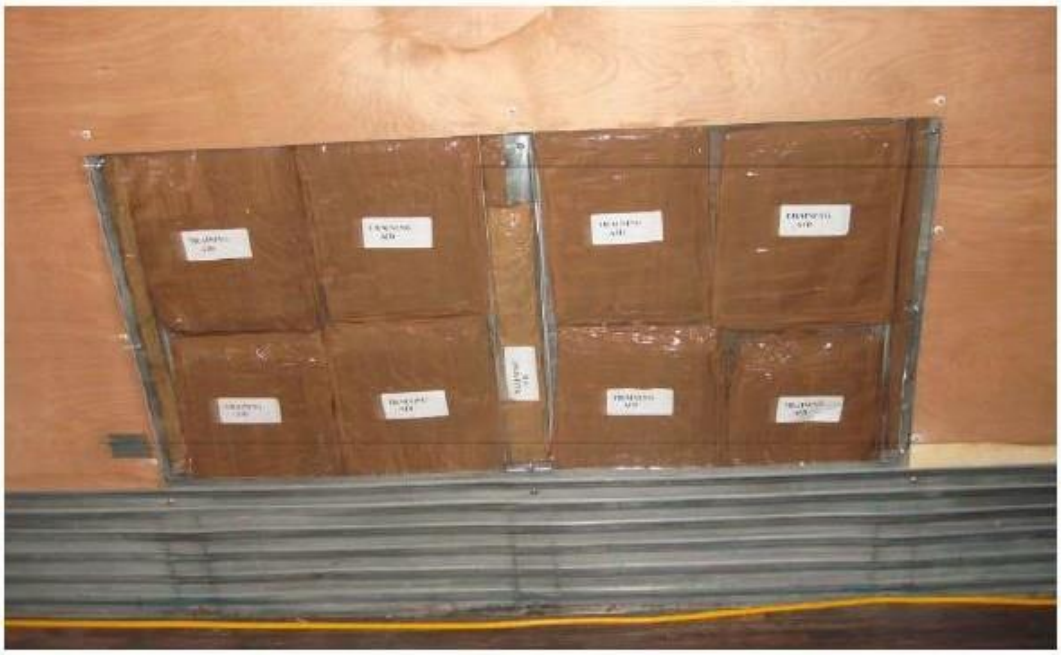
1. There will be visual indications that an area has been disturbed or altered and employees must be trained to recognize it.
2. It is important to have good recognition of normal factory construction, normal oxidation, and dirt accumulation from normal use so that indicators of tampering or alterations can be spotted.
3. Be systematic in your search for evidence of tampering. Have documented procedures that all inspection personnel follow.
4. Use the 7-point inspection method for containers.
5. Use the V-V-T-T method for seal inspection. (View, verify, tug, twist)
6. Tap the walls, ceiling, doors, and floor with a metal tool to listen for hollow cavities where contraband might be stored.

Examples of Altered Containers and Hidden Contraband

False Floor

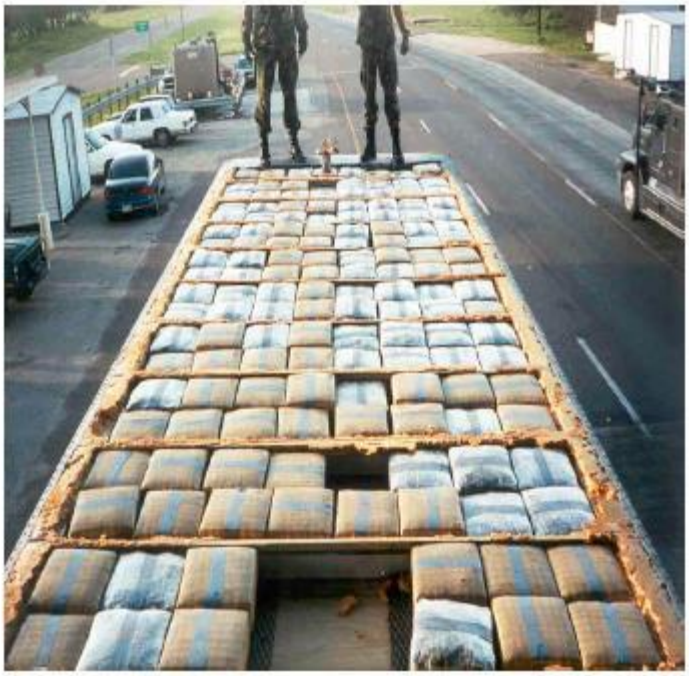


Side Walls

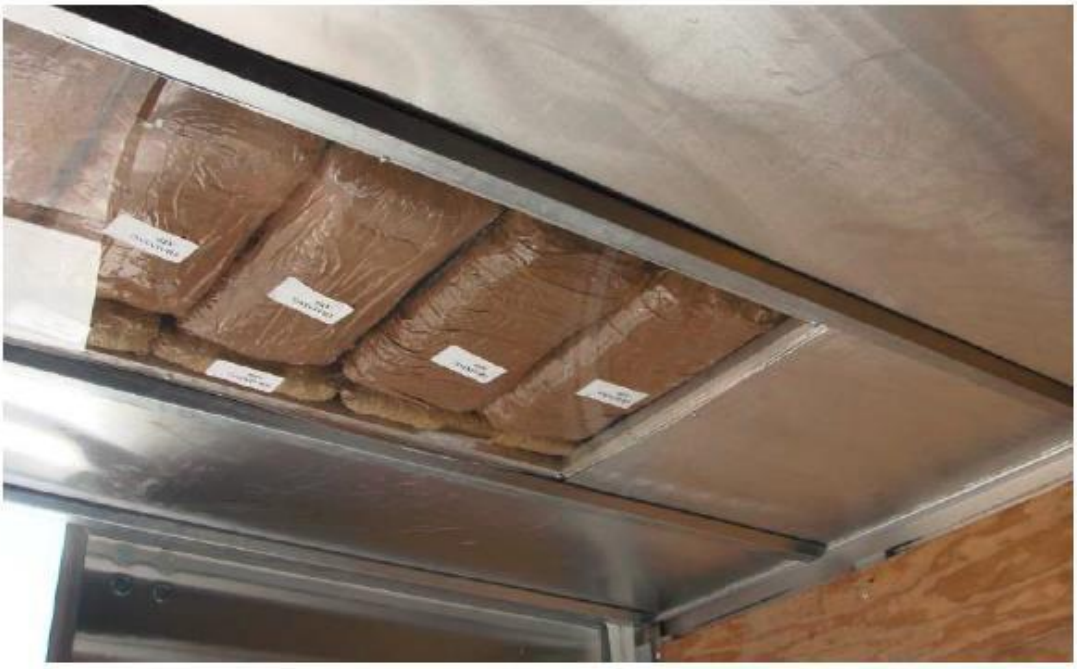


Contraband in False Wall

Roof Compartments



Roof Compartments



Inspection Points

Look for these indications of tampering or alteration:

1. Scratches
2. Burn/Weld Marks
3. Tampered Bolts/Rivets
4. Fresh Grease
5. Fresh Paint
6. Silicone
7. Fiberglass Patchwork
8. Odor Masking Substances
9. After Market Modifications
10. Hollow Sounding Cavities (strike surfaces with a metal tool)

Factory CTPAT Security Criteria – Summary with Translation

Factories must implement minimum security criteria and best practices to help secure our supply chain from terrorist activity. The criteria are based on a set of recommendations developed as a result of the Customs Trade Partnership Against Terrorism (CTPAT) initiative with US importers.

Key Requirements

Factory Security requires that all vendor and factory partners producing merchandise for The Pep Boys:

1. Take all necessary precautions to ensure against the introduction of unauthorized material and/or persons into containers and trailers.
2. Prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets.
3. Have processes in place to screen prospective employees, and to periodically check current employees.
4. Create procedures to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain.
5. Have IT security policies, procedures and standards in place.
6. Employees must be offered specific training in how to maintain cargo integrity, recognize internal conspiracies, and protect access controls.
7. Have a documented and verifiable process for determining risk throughout their supply chain.

Indicators of Noncompliance

1. Lack of perimeter fencing, guard stations, or security personnel to prevent unauthorized entry to the cargo handling and storage area of the facility.
2. Lack of locking mechanisms on containers and trailers, facility windows and doors, or perimeter fencing.

3. Ability to enter production facility without proper documentation, and visit without an escort.
4. Employees are hired without verification of employment history, or background checks.
5. No controls exist to identify shortages, overages, or other significant cargo discrepancies.

Good Management Practices

1. Before a prospective employee is hired a background check is conducted, and employment history and references are verified.
2. A high security seal is affixed to all loaded containers and trailers bound for the US.
3. Employees have limited access to keys, key cards, and computer systems unless they have a job related to the need for such access.
4. Visitors present photo identification upon arrival and all visitors are escorted and display visible temporary identification.
5. Arriving packages and mail is periodically screened before being disseminated.
6. Departing cargo is reconciled against information on the cargo manifest and purchase order.
7. Drivers delivering or receiving cargo are positively identified before cargo is received or released.
8. Cargo handling and storage areas have physical barriers and deterrents that guard against unauthorized access.
9. A threat awareness program is established to foster employee education on the threat posed by terrorists and contraband smugglers at each point in the supply chain.
10. The facility has adequate lighting inside and outside the facility, including parking areas.
11. The factory has established procedures to conduct periodic unannounced checks related to personnel security, information access control, shipment information control, storage and distribution security, contractor controls, and education and awareness.

供应链安全（**C-TPAT**） 工厂须执行基本的安全保障标准，以确保供应链免于恐怖主义活动。该标准 需建 立于美国进口商编订的海关及贸易伙伴反恐建议。

主要规定

“供应链安全”条款为 The Pep Boys 的所有供应商及生产厂家制定了以下 主要规定：

•采取一切必要的预防措施以禁止未被授权的物或人进入货柜车和拖车。

•经授权方可进入厂区，保持对雇员和访客的出入进行有效控制，保护公司资产。

•建立员工招聘程序，并定期对在职员工进行审查。

•建立相关程序确保货物在运输、处理和贮存过程中的完整性与安全性。

•建立相关 **IT** 信息安全政策、程序和标准。

•为员工提供有关货物完整性维护，内部阴谋识别和授权管制方面的培训。

•建立文件化的程序以识别供应链存在的潜在安全风险。

违规行为

•货物处理及贮存区域未设立栅栏，或保安岗位，或安全保卫人员以管制未经授权的进入。

•货柜车、拖车和厂区门窗及栅栏未安装锁具。

•未经文件授权和陪同，非法进入生产区域。

•招聘员工时未进行入职前的履历和背景调查。

•未监管货物的短装、过剩或其它明显偏差。

良好管理实务

•招聘员工以前对其背景，雇员履历以及推荐信等进行审查。

•在所有出货至美国的货柜车及拖车粘贴高安全性能的封条。

•有关职能人员方可授权使用钥匙、钥匙卡以及电脑系统。

•访客来访须出示带有相片的身份证明，所有访客须有人陪护，且出示临时访客证。

•定期筛查来往包裹和电邮。

•出货时先核对出货单及订单。

•负责送货/收货的司机持有确定身份证明。

•货物处理及贮存区域设立栅栏或障碍以控制未经授权的进入。

•为员工提供安全威胁意识方面的培训，让员工了解恐怖主义和非法走私对供应链的威胁。

•厂区内外，包括停车场，配备足够的照明。

•建立内部稽查程序，定期对人员安全，资讯控制，船务控制，仓储安全，分包商控制和安全意识培训的措施执行进行突击檢查。

最终文本（2006 年 8 月 29 日）

海关-商业伙伴反恐计划（C-TPAT）

外国制造商安全标准

本最低安全标准是为使外国制造商实施高效安全实务以优化供应链的绩效，从而减少恐怖分子 以及恐怖主义的实施行为通过丢失、盗窃和走私货物渗入全球供应链的危险而设计的基本结构单元 。 犯罪团伙通过内部阴谋破坏世界商贸活动的倾向和活动范围要求公司，尤其是外国制造商，提高它 们的安全实务。 外国制造至少必须每年一次，或者根据情况的需要，比如在高度警戒、发生安全违反或安全事 故的期间，根据下面所述的 C-TPAT 安全标准对它们的国际供应链进行全面评估。如果外国制造商 将它们供应链的某些部分外包或承包给比如另一个外国机构、仓库或其他部门，则外国制造商必须 与这些商业伙伴一起确保在整个供应链中相关的安全措施都得以实施和遵守。C-TPAT 所定义的供应
链是支从原发点（制造商/供应商/卖主）一直到销售点的整个过程，并且适用于 C-TPAT 成员所使用 的各种不同的
商业模式。

C-TPAT 认识到国际供应链以及安全实务的复杂性，并且支持基于风险的存在而对安全措施的应用和实施注 1。因此，本计划允许基于成员的商业模式而灵活实施客户化的安全计划。 本文所列举的适当的安全措施必须基于风险的性质在外国制造商的整个供应链中得以实施和维 持注 2。

商业伙伴要求 外国制造商对于商业伙伴的选择，包括承运人、其他制造商、产品供应商和卖主（零件和原材 料供应商等）必须有书面的、可核准的程序。

安全程序

对于那些符合 C-TPAT 认证条件的商业伙伴（承运人、进口商、港口、码头、经纪人、并装业者等），外国制造商必须有文件证据（比如 C-TPAT 证书、SVI 编号等）表明这些商业伙伴是否经过 C-TPAT 认证。

对那些不符合 C-TPAT 认证条件的商业伙伴，外国制造商应要求它们的商业伙伴出示它们达到 C-TPAT 安全标准的书面/电子确认书（比如合同义务；由商业伙伴的一位高级官员签字保证合规的信件；由商业伙伴出示一份书面声明表明其符合 C-TPAT 安全标准或一个外国海关主管部门管理为世界海关组织（WCO）所认可的同等安全计划的要求；或者，提供一份完整的外国制造商安全问卷）。基于一项被记录的风险评估程序，外国制造商必须对不符合 C-TPAT 条件的商业伙伴进行核准，以验证其是否达到 C-TPAT 的安全标准。

原发点

外国制造商必须确保商业伙伴遵照 C-TPAT 安全标准制定安全程序和规程，以强化在原发 点装运、组装或制造的完整性。基于风险的性质应对商业伙伴的程序和设施定期进行审核，

并且保持外国制造商所要求的安全标准。

参与外国海关主管机关的供应链安全计划及获得认证的情况 获得外国海关主管机关管理的供应链安全计划认证的当前或未来的商业伙伴应被要求向 外国制造商表明其参与计划的状况。

安全程序

对于运往美国的货物，外国制造商应监督将运输服务分包给其他承运人的 C-TPAT 承运人用的是其他为 C-TPAT 所批准的承运人，或者如果是非 C-TPAT 批准的承运人，则其达到商业伙伴要求里所描述的 C-TPAT 安全标准。 因为外国制造商须对将货物装运上拖车或集装箱负责，因此它们应该与承运人一起工作以 确保在装运时实施了有效的安全程序和控制措施。

1．外国制造商应基于它们的商业模式对它们整个供应链中存在的风险应该有记录在案的、可核准的确定程序（运输量、原产国、航线、C-TPAT 成员资格、通过公开信息渠道获悉的潜在恐怖威胁、存在的安全隐患、过去的安全事故等）。

2．外国制造商应基于它们的商业模式对它们整个供应链中存在的风险应该有记录在案的、可核准的确定程序（运输量、原产国、航线、C-TPAT 成员资格、通过公开信息渠道获悉的潜在恐怖威胁等）。

2

最终文本（2006 年 8 月 29 日）

集装箱及拖车的安全 集装箱及拖车的完整性应得到维护以确保不会混入未经许可的物品和/或人。在装运货物的时候， 应该有恰当地贴封条和保持装运集装箱和拖车的完整性的程序。所有运往美国的装有货物的集装箱 和拖车都必须贴上高度安全封条。所有封条都必须符合或超出现行 PAS ISO 17712 对高度安全封条 的标准。 在风险评估有理由要求检查集装箱或拖车是否藏匿有人员或走私货物的地理区域，在制造场所 或装运地应该有检查是否存在该等风险的程序。

集装箱检查 在装运前应该有查验集装箱结构物理完整性的程序，包括门的锁闭系统的可靠性。本计划 建议对所有集装箱进行如下七点检查程序：

前壁 左

侧 右侧

地板 顶

部 内/外

门

外部/起落架

拖车检查

在装运前应该有查验拖车结构物理完整性的程序，包括门的锁闭系统的可靠性。本计划建议对所有集装箱进行如下七点检查程序：

第五轮区域——检查自然隔间/车底护板

外部——前面/侧面

尾部——保险杠/门

前壁

左侧 右

侧 地板

顶部 内/

外门

外部/起落架 集装箱

及拖车的封条

集装箱和拖车的封条，包括封条持续的完整性，是一条安全的供应链的重要组成部分，并且是外国制造商忠实执行 C-TPAT 计划的关键部分。外国制造商必须给所有运往美国的装有货物的集装箱和拖车贴上高度安全封条。所有封条都必须符合或超出现行 PAS ISO 17712 对高度安全封条的标准。 应该制定有书面的程序规定对封条的管理以及如何贴到装有货物的集装箱和拖车上，包 括识别和向美国海关和边境保护局或适当的外国主管部门报告受损的封条和/或集装箱/ 拖车的程序。只有被指定的雇员才能分发表示完整性的封条。

集装箱和拖车的存放 受外国制造商控制或位于外国制造商场所的集装箱和拖车必须被存放在安全的区域以免 有未经许可的人员进入和/或篡改。应该有报告和解决未经许可擅自进入集装箱/拖车或集装箱

/拖车的存放区域的程序。 物理进入控制 进入控制用来防止未经许可进入设施的现象，维持对雇员和来访者的控制以及保护公司的财 产。进入控制必须包括在所有的进入点对所有雇员、来访者和卖主的积极识别。

雇员 应该安装雇员识别系统以便进行积极的识别和进入控制。只有确有工作需要的人才能被 允许金融安全区域。公司管理人员或安全人员必须对雇员、来访者和卖主的识别标志的发放 和回收进行恰当的控制。发放和回收识别标志以及更换进入手段（比如钥匙、钥匙卡等）的 程序必须被记录在案。

来访者

来访者在抵达时必须出示带有照片的身份证明以作记录。所有来访者都必须有人陪同，并且必须可视地展示临时性的识别标志。

交货（包括邮件） 所有卖主在抵达时必须出示适当的卖主身份和/或带有照片的身份证明以作记录。所有运 达的包裹和邮件在散发出去前必须定期进行检查。

质询及将未经许可进入的人员带离现场
应该有识别、质询和确认未经许可进入/身份不明的人员的程序。
个人安全 应该有审查预期雇佣的雇员和定期审查现有雇员的程
序。

雇佣前审核 在雇佣员工前应审核申请表信息，比如雇员的工作
经历和推荐信。

背景检查/调查 对于预期雇佣的雇员应按照外国法规的规定检查和调查其背景情况。
在雇佣员工后，应 根据事情的原由和/或雇员职位的敏感性对其进行定期检查和调查。

个人离职程序 公司对于离职的雇员必须有去除身份证明标志、设备和进入
系统设施的程序。 程序安全
应该制定有确保供应链中货物在运输、搬运和存放过程中的完整性和安全性的安全措施。

文档程序
应该制定有程序确保用于商品/货物清理的所有信息易读、完整、准确以及不会被更改、
丢失或引入错误的信息。文档控制必须包括保护计算机不被擅自闯入以及保护计算机信
息的程序。

报告程序 为确保货物的完整性，必须有确保从商业伙伴处接收到的信息被准确和及时
报告的程序。

装运和接收货物 被装运后将要离岸的货物应该与货物单的信息相符。货物应该被准
确地描述，重量、标
签、标记和件数应被列明和核准。离岸的货物应该与购货订单或装运订单上的内容进行
校对。在货物被接收或发放前应对装运或接收货物的驾驶员进行积极的身份认定。同时
还应该建立跟踪进出货物及时动向的程序。

货物差异 所有货物的短缺、超额和其他重大的差异或异常情况都必须得到合理的解
决和/或调查。 如果发现有异常情况、非法或可疑活动，必须报告海关和/或其他适当的
执法机关。 物理安全
位于国际场所的货物搬运和存放设施必须安置有物理障碍物和制止物以阻止人员未经许可进入
里面。在适用的范围内，外国制造商应在它们的供应链中始终遵循以下的 C-TPAT 物理安全标准。

围栏
货物搬运和存放设施的区域四周必须用围栏包围起来。货物搬运装置应该有内部围栏以
将国内、国际、高价值和危险品货物隔离开。所有的围栏都必须经常检查其完整性及是
否有损坏现象。

大门和门房 车辆和/或人员进出的大门应该有人把守和/或被监视。大门的数量应该在
保证适当进出和
安全的基础尽可能保持最少。

停车场

私人载客车辆应被禁止进入停车场或临近货物搬运和存放区域。

建筑物

建筑物的建筑材料应能阻止非法进入。通过定期检查和维修保持建筑物的完整性。

锁闭装置和钥匙控制

所有外部和内部的窗子、大门和围栏都必须有锁闭装置以确保安全。管理人员或安全人员必须控制所有锁和钥匙的发放。

照明 在设施的内部和外部应该有适当的照明设施，包括在以下一些区域：进口和出口、货物 搬运和存放区域、围栏线和停车场。

警报系统和监视摄像头 应该安装警报系统和监视摄像头以监视货物搬运和存放场所以及防止未经许可的人员进 入货物搬运和存放区域。

信息技术安全

口令保护

自动化系统必须使用需要定期更换口令的个人担保账户。必须制定并实施信息技术安全政策、程序和标准，同时应对雇员进行培训。

解释责任 必须有识别滥用信息技术，包括不当进入、干扰或篡改商业数据的体系。所有扰乱系统

的人都必须因其滥用信息技术的行为而受到适当的纪律处分。

安全培训及忧患意识

安全人员应该制定并保持一项忧患意识计划以便识别以及培养对供应链的各个点上恐怖分子和 走私者所带来的威胁的意识。雇员必须了解公司应对某种状况以及如何进行报告的程序。对在装运和接收货物领域工作以及接收和打开信件的雇员应该进行额外的培训。 此外，应该提供特定的培训以帮助雇员保持货物的完整性、识别内部阴谋以及保护进出控制。 这些计划应该给积极参与的雇员提供奖励。

Pep Boys Foreign Vendor CTPAT Security Survey

2017

Version 7.0
Updated October 2017

Index

Introduction

Pep Boys is committed to a safe and secure supply chain by participating in CTPAT (Customs-Trade Partnership Against Terrorism), a voluntary United States Customs and Border Protection business initiative designed to build cooperative relationships to strengthen the supply chain and border security and to continue the free flow of international trade. Pep Boys received its CTPAT certification in January 2009 from U.S. Customs and was moved to Tier III status on December 30, 2014; the highest level of participation. We ask that all our Business Partners assist us in securing our supply chain.

Part of our CTPAT certification requires Pep Boys to identify which of its business partners are now, or plan to be CTPAT certified. All business partners who are not members must demonstrate a commitment to meeting the minimum-security requirements appropriate to their business, including Container/Trailer Security (seals, inspections, and storage), Procedural Security, Physical Security, Personnel Security, Access Control, Security, Threat Awareness Training, and Business Partner Screening.

A completed Factory Information (page 27) and CTPAT Minimum Security Survey (Pages 28-36) for each factory where Pep Boys products are manufactured, consolidated, or stored is required to evaluate your compliance and commitment to CTPAT requirements.

The CTPAT Minimum Security Survey (Pages 28-36) must be read carefully and filled out completely by each factory or facility. A simple Yes or No answer is not sufficient; details must be given for each answer on the lines provided. If details are not provided the manual will be sent back to be filled out completely.

Please see the document titled "Foreign Vendor CTPAT Security Manual" for information regarding CTPAT's requirements and training material to distribute to your employees. Do not hesitate to contact us with any questions or for additional training and information.

Additional information regarding CTPAT can be found by visiting the U.S. Customs and Border Protection site at: http://www.cbp.gov/.

Thank you for your cooperation,
The Pep Boys – Manny, Moe & Jack

Contacts

Martina Gring
Logistics Specialist
The Pep Boys - Manny, Moe & Jack
Phone: 215-430-9430
Email: Martina_Gring@Pepboys.com

George Pavlichko
Director of Global Logistics
The Pep Boys - Manny, Moe & Jack
3111 West Allegheny Ave.
Philadelphia, PA 19132
Phone: 215-430-9059
Email: George_Pavlichko@Pepboys.com

This document must be completed annually. Please read carefully and fill out completely. This document can be typed or printed and hand written.

Factory Information

1. **Factory Name:** _____
2. **Country:** _____
3. **Region:** _____
4. **Postal Code:** _____
5. **Closest Ocean Port (FOB):** _____
6. **Number of workers:** _____
7. **Primary Contact Name:** _____
8. **Primary Email Address:** _____
9. **Primary Phone Number:** _____
10. **Primary Fax Number:** _____
11. **Years at current location:** _____

CTPAT Minimum Security Requirements Survey

This document must be filled out completely by each factory or facility where Pep Boys products are manufactured, consolidated or stored on an annual basis.

Please circle your answer 'Yes' or 'No'. If you answered 'Yes' please provide details on the lines below each question. **This is a requirement. Any assessments received by Pep Boys without details for ALL questions will be returned for completion.**

US Company Name: _____

Factory Name: _____

CTPAT and Supply Chain Security Programs

1. Are you currently a member of CTPAT?

Yes **No**

If yes, please provide your Status Verification Interface (SVI) number:

_____
_____
_____

2. Have you obtained a certification in a supply chain security program being administered by another foreign Customs Administration?

Yes **No**

If yes, please indicate the name of the program and your status of participation:

_____
_____
_____

Physical Security

1.

a. Does your facility have a fence that secures the entire perimeter including the shipping and receiving area?

Yes **No**

If yes please describe:

_____
_____
_____

b. If yes, is that fence topped with barbed wire or any other trespassing deterrent?

Yes **No**

If yes please describe:

_____
_____
_____

2. Is the fence and gate kept securely locked when not in use?

Yes **No**

If yes please describe:

_____
_____
_____

3. Is the fence and gate monitored by a guard house?

Yes **No**

If yes please describe:

_____
_____
_____

4. Is the building made of cement or other equal building material?

Yes **No**

If yes please describe:

_____
_____
_____

5. Do all windows and doors have locks?

Yes **No**

If yes please describe:

_____
_____
_____

6. Do the interior, exterior, and loading areas have adequate lighting?

Yes **No**

If yes please describe:

_____
_____
_____

7. Are there security cameras and alarm systems installed along the perimeter and restricted access areas of the facility?

Yes **No**

If yes please describe:

_____
_____
_____

Container Security

1. Are the containers loaded in a secure fenced in area on your premises?

Yes **No**

If yes please describe:

_____
_____
_____

2. Are the containers inspected for damage prior to loading?

Yes **No**

If yes please describe:

_____
_____
_____

3. Are the trailers inspected for damage or abnormalities prior to the container drayage?

Yes **No**

If yes please describe:

_____
_____
_____

4. Are seals kept in a secure area and their use monitored?

Yes **No**

If yes please describe:

_____
_____

_____

5. Is a record kept of the seals used?

Yes **No**

If yes please describe:

_____
_____
_____

Physical Access Controls

1. Are employees positively identified by security personnel when entering the premises?

Yes **No**

If yes please describe:

_____
_____
_____

2. Do the employees have ID badges to enter the premises?

Yes **No**

If yes please describe:

_____
_____
_____

3. Are visitors identified upon entrance, given a visitor's badge, and escorted during their visit?

Yes **No**

If yes please describe:

_____
_____
_____

4. Are delivery identified and their packages inspected?

Yes **No**

If yes please describe:

_____
_____
_____

5. Is there a process to identify, challenge and remove unauthorized/unidentified persons from the premises?

Yes **No**

If yes please describe:

_____
_____
_____

Personnel Security

1. Are prospective employees given background checks?

Yes **No**

If yes please describe:

_____

_____

_____

2. Are prospective employees' references checked prior to employment?

Yes **No**

If yes please describe:

_____

_____

_____

3. Are there procedures in place to de-brief terminated employees such as removing their computer access and collecting company issued ID badges?

Yes **No**

If yes please describe:

_____

_____

_____

Procedural Security

1. Are documents (Bills of Lading, Packing List, Commercial Invoice, Container Manifest, etc) audited for their integrity and completeness?

Yes **No**

If yes please describe:

_____
_____
_____

2.Are the documents completed at least 24 hours prior to container delivery to the pier?

Yes **No**

If yes please describe:

_____
_____
_____

3.Are cargo descriptions including weight, pieces, and marks verified prior to loading the container?

Yes **No**

If yes please describe:

_____
_____
_____

4.Are drivers positively identified via ID badges or Driver's Licenses when picking up the containers for delivery?

Yes **No**

If yes please describe:

_____
_____
_____

5.Are shortages, overages, and anomalies investigated and resolved?

Yes **No**

If yes please describe:

_____
_____
_____

Information Technology Security

1.Are passwords required to log in to company databases and computer systems?

Yes **No**

If yes please describe:

_____

_____

_____

2. Is the company's computer system protected by a firewall?

Yes **No**

If yes please describe:

_____

_____

_____

Security Training and Threat Awareness

1. Are there procedures in place in the event security is compromised at your facility?

Yes **No**

If yes please describe:

_____

_____

_____

2. Are employees properly trained to follow these procedures?

Yes **No**

If yes please describe:

_____

_____

_____

3. Do employees or security personnel perform periodic testing of all security measures related to transportation (alarm systems, security cameras, etc)?

Yes **No**

If yes please describe:

_____

_____

_____

4. Are there incentives for employees to participate in your security program? i.e. rewards for reporting suspicious activity)

Yes **No**

If yes please describe:

_____

_____

_____

Business Partner and Sub Contractor Screening

1. Are potential business partners and sub-contractors screened and verified?

Yes **No**

If yes please describe:

_____

_____

_____

Completed By (Print or Type): _____

Company: _____

Title or Position: _____

Signature: _____

Date: _____

CTPAT MINIMUM SECURITY SURVEY FOLLOW UP

Upon review of your security survey Pep Boys will advise on any deficiencies in the security of your facility. Pep Boys will work with you to improve your security to ensure that your facility meets CTPAT's minimum security criteria. Please see the document titled "Foreign Vendor CTPAT Security Manual" for information regarding CTPAT's requirements and training material to distribute to your employees.

Pep Boys may request further clarification or documentation on specific survey answers.
