Genesco

GENESCO Inc.’s C-TPAT Security Expectations for Vendors and Manufacturers

CTPAT

YOUR SUPPLY CHAIN'S STRONGEST LINK.

Introduction

In direct response to 9/11, the U.S. Customs Service, now U.S. Customs and Border Protection (CBP) challenged the trade community to partner with CBP to design a new approach to supply chain security focused on protecting the United States against acts of terrorism by improving security while simultaneously speeding the flow of compliant cargo and conveyances. The result was the Customs-Trade Partnership Against Terrorism (C-TPAT) – an innovative, voluntary government/private sector partnership program.

C-TPAT builds on the best practices of CBP/industry partnerships to strengthen supply chain security, encourage cooperative relationships and to better concentrate CBP resources on areas of greatest risk. It is a dynamic, flexible program designed to keep pace with the evolving nature of the terrorist threat and the changes in the international trade industry, thus ensuring the program's continued viability, effectiveness and relevance. Flexibility and customization are important characteristics of C-TPAT.

Genesco Inc. became a certified C-TPAT member in 2003. Genesco Inc. is committed to keeping our supply chain secure to agreed security standards through self-policing and implementing changes as needs arise. The current security guidelines for C-TPAT program members address a broad range of topics including personnel, physical and procedural security; access controls; education, training and awareness; manifest procedures; conveyance security; threat awareness; and documentation processing. Companies that apply to C-TPAT must sign an agreement with CBP that commits their organization to the program's security guidelines. These guidelines offer a customized solution for the members, while providing a clear minimum standard that approved companies must meet.

In mid-2019, CBP published updated Minimum Security Criteria (MSC) to reflect new and evolving threats and challenges facing supply chain today. Each of the "Focus Areas" below have had some form of change, including expanding implementation guidance as well newly added "Criteria Categories" such as those to security technology, cybersecurity and agricultural security.

Focus Areas	Criteria Categories
Corporate Security	1. Security Vision and Responsibility (New category)
	2. Risk Assessment
	3. Business Partner Security
	4. Cybersecurity (New category)
Transportation Security	5. Conveyance and Instruments of International Traffic Security
	6. Seal Security
	7. Procedural Security
	8. Agricultural Security (New category)
People and Physical Security	9. Physical Access Controls
	10. Physical Security
	11. Personnel Security
	12. Education, Training, and Awareness

For additional information, please visit US Custom's CTPAT website link below:
https://www.cbp.gov/border-security/ports-entry/cargo-security/CTPAT

CTPAT FOREIGN MANUFACTURER'S MINIMUM SECURITY CRITERIA

Genesco, Inc. is implementing the following requirements to reflect CBP's roll-out of the updated MSC.

REQUIREMENTS: All vendors and their respective factories must have the following procedures in place. Procedures must be in written documentation and provided to Genesco. This is applicable for both CFS load and factory-load vendors.

IMPORTANT NOTE: If not otherwise specifically indicated, "periodic" or "periodically" referenced is not meant to allow to be interpreted as an annual, once a year, review. Instead, vendor/factory must set more frequent "periodic" audits such as every 3 months or more/less as needed. Security risks monitoring is a constantly changing reality. Vendors needs to apply the usage of periodic internal auditing or reviews as necessary for each area in order to ensure that their processes are working as documented and intended.

If there are any questions, please contact GlobalCompliance@genesco.com

Table of Contents

Focus Area #1: Corporate Security

Corporate Security Focus Area Requirements:

I. Security Vision & Responsibility

Vendor and factory leadership is fully responsible and supportive of implementing an effective supply chain security program. Leadership should instill security as an integral part of the company's culture and ensuring that it is a companywide priority.

Vendor/Factory requirements:

A. Statement of support from leadership

i. Statement of support issued and signed by senior leadership such as President, CEO, General Manager, or Security, highlighting the importance of protecting the supply chain from criminal activities such as drug trafficking, terrorism, human smuggling, and illegal contraband.

ii. Areas to display the statement of support include the company's website, on posters in key areas of the company (reception; packaging; warehouse; etc.), and/or be part of company security seminars, etc.

B. Build a cross-functional team as part of your Supply Chain Security Program

i. To build a robust Supply Chain Security Program, a company should incorporate representatives from all of the relevant departments into a cross-functional team including but not limited to traditional Security, Human Resources, Information Technology, and Import/Export departments.

C. Conduct written reviews of your Supply Chain Security Program

i. The supply chain security program must be designed with, supported by, and implemented by an appropriate written review component. The purpose of this review component is to document that a system/process is in place whereby personnel are held accountable for their responsibilities and all security procedures outlined by the security program are being carried out as designed. The review plan must be updated as needed based on pertinent changes in an organization's operations and level of risk. Vendors and/or factories must conduct targeted reviews at least annually, but recommended to be conducted quarterly, to ensure all areas of the supply security program is working as designed – e.g. container and conveyance inspections, seal controls, incoming package scanning, employee background checks, etc.

D. Keep leadership informed

i. Vendor and/or factories must assign a point of contact, which must stay knowledgeable about CTPAT program requirements.

ii. Point of contact must provide regular updates to upper management on issues related to the program, including the progress or outcomes of any audits, security related exercises, and CTPAT validations.

II. Risk Assessment

The continuing threat of terrorist groups and criminal organizations targeting supply chains underscores the need for vendors and factories to assess existing and potential exposure to these evolving threats.

Key Definition:

Risk – A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence. What determines the level of risk is how likely it is that a threat will happen. A high probability of an occurrence will usually equate to a high level of risk. Risk may not be eliminated, but it can be mitigated by managing it – lowering the vulnerability or the overall impact on the business.

Vendor/Factory requirements:

A. Document risk assessments

i. Vendors and factories must review and document the overall risk assessment (RA) to identify where security vulnerabilities may exist within their supply chain. The RA must identify threats, assess risks, and incorporate sustainable measures to mitigate vulnerabilities.

B. Map vendor/factory supply chain

i. Vendors and factories should map how cargo moves in and out of transport facilities/cargo hubs and noting if the cargo is "at rest" at one of these locations for an extended period of time.

ii. The mapping should consider all applicable involved parties- including those who will only be handling the import/export documents such as customs brokers and others that may not directly handle the cargo but may have operational control such as Non-Vessel Operated Common Carriers (NVOCCs) or Third-Party Logistics Providers (3PLs).

iii. If any portion of the transport is subcontracted, this may also be considered because the more layers of indirect parties, the greater risk involved.

C. Conduct annual risk assessments

i. Risk assessments must be reviewed annually, or more frequently as risk factors dictate.

D. Require crisis management, business continuity, and business recovery plans

i. Vendors and factories should have written procedures in place that address crisis management, business continuity, security recovery plans, and business resumption.

ii. A crisis may include the disruption of the movement of trade data due to a cyberattack, natural disasters such as fire, flooding and etc., or a carrier driver being hijacked by armed individuals. Based on risk and where the vendor/factory operates or sources from, contingency plans may include additional security notifications or support; and how to recover what was destroyed or stolen and get back to normal operating conditions.

III. Business Partners

Vendors and factories and their respective business partners that directly handle cargo and/or import/export goods and documentation, must have appropriate security measures in place to secure the goods throughout the international supply chain.

When business partners subcontract certain functions, an additional layer of complexity is added to the equation, which must be considered when conducting a risk analysis of a supply chain.

Key Definition:

Business Partner – A business partner is any individual or company whose actions may affect the chain of custody security of goods being imported to or exported from the United States via a CTPAT Member's supply chain. A business partner may be any party that provides a service to fulfil a need within a company's international supply chain.

These roles include all parties (both direct and indirect) involved in the purchase, document preparation, facilitation, handling, storage, and/or movement of cargo for, or on behalf, of a CTPAT Importer or Exporter Member.

*Examples of a vendor or factory's indirect business partners would be subcontracted truckers to move cargo, out-sourced security guards working in the factories and other logistics carriers and overseas consolidation warehouses – arranged for by an agent/logistics provider.

Vendor/Factory requirements:

A. Require business partner screening to align with CTPAT MSCs

i. Vendors and factories must have a written, risk-based process for screening new business partners and for monitoring current partners. A factor that vendor/factories should include in this process is checks on activity related to money laundering and terrorist funding.

ii. The following are examples of some of the vetting elements that can help determine if a company is legitimate:

1. Verifying the company's business address and how long they have been at that address;
2. Conducting research on the internet on both the company and its principals;
3. Checking business references; and
4. Requesting a credit report.

iii. Examples of business partners that need to be screened are direct business partners such as manufacturers, product suppliers, pertinent vendors/service providers, and transportation/logistics providers. Any vendors/service providers that are directly related to the company's supply chain and/or handle sensitive information/equipment are also included on the list to be screened; this includes brokers or contracted IT providers.

B. Review business partners for any foreign AEO/CTPAT equivalent certification credentials

i. The vendor/factories' business partner screening process must take into account whether a partner is a CTPAT Member or a member in an approved Authorized Economic Operator (AEO) program with a Mutual Recognition Arrangement (MRA) with the United States (or an approved MRA). Certification in either CTPAT or an approved AEO is acceptable proof for meeting program requirements for business partners.

ii. If vendor/factory has obtained certification from a foreign AEO program under an MRA with the United States, the foreign AEO certification proof should be submitted to Genesco.

iii. Vendors/factories may visit the foreign Customs Administration's website where the names of the AEOs of that Customs Administration are listed or request the certification directly from their business partners.

iv. Current United States MRAs include: New Zealand, Canada, Jordan, Japan, South Korea, the European Union (28 Member States), Taiwan, Israel, Mexico, Singapore, the Dominican Republic, and Peru.

C. Due diligence on outsourced business partners to ensure they adhere and continue to comply with CTPAT MSC

i. Where a vendor or factory outsources or contracts elements of its supply chain, the vendor/factory must exercise due diligence (via visits, questionnaires, documented process, contractual agreement etc.) to ensure these business partners have security measures in place that meet or exceed CTPAT's Minimum Security Criteria (MSC).

ii. To verify adherence to security requirements, vendors/factories must conduct security assessments of their business partners. This should be done minimum annually if the same contractor is used, or as risks dictate.

iii. Determining if a business partner is compliant with the MSC can be accomplished in several ways. Based on risk, the company may conduct an onsite audit at the facility, hire a contractor/service provider to conduct an onsite audit, or use a security questionnaire. If security questionnaires are used, the level of risk will determine the amount of detail or evidence required to be collected. More details may be required from companies located in high-risk areas. If a vendor/factory is sending a security questionnaire to its business partners, consider requiring the following items:

1. Name and title of the person(s) completing it;
2. Date completed;
3. Signature of the individual(s) who completed the document;
4. *Signature of a senior company official, security supervisor, or authorized company representative to attest to the accuracy of the questionnaire;
5. Provide enough detail in responses to determine compliance; and
6. Based on risk, and if allowed by local security protocols, include photographic evidence, copies of policies/procedures, and copies of completed forms like Instruments of International Traffic inspection checklists and/or guard logs.

*Signatures may be electronic. If a signature is difficult to obtain/verify, the respondent may attest to the questionnaire's validity via email, and that the responses and any supporting evidence was approved by a supervisor/manager (require name and title).

D. Addresses security/MSC weaknesses as soon as possible

i. If weaknesses are identified during business partners' security assessments, they must be addressed as soon as possible, and corrective action plan must be implemented in a timely manner. Vendor/factories must confirm that deficiencies have been mitigated via documentary evidence.

ii. CTPAT recognizes that there will be different timelines for making corrections based on what is needed for the correction. Installing physical equipment usually takes longer than a procedural change, but the security gap must be addressed upon discovery. For example, If the issue is replacing a damaged fence, the process to purchase a new fence needs to start immediately (addressing the deficiency) and the installation of the new fence (the corrective action) needs to take place as soon as it is feasible.

iii. Based on the level of risk involved and the importance of the weakness found, some issues may require immediate attention. If it is a deficiency that may jeopardize the security of a container, for instance, it should be addressed as soon as possible.

iv. Some examples of documentary evidence may include copies of contracts for additional security guards, photographs taken of a newly installed security camera or intrusion alarm, or copies of inspection checklists, etc.

E. Keep security assessments up-to-date

i. To ensure their business partners continue to comply with CTPAT's security criteria, Vendor/factories should update their security assessments of their business partners on a regular basis, or as circumstances/risks dictate.

ii. Periodically reviewing business partners' security assessments is important to ensure that a strong security program is still in place and operating properly. If a vendor/factory never required updates to its assessment of a business partner's security program, the vendor/factory would not know that a once viable program was no longer effective, thus putting the vendor/factory's supply chain at risk.

iii. Deciding on how often to review a partner's security assessment is based on the vendor/factory's risk assessment process. Higher risk supply chains would be expected to have more frequent reviews than low risk ones. If a vendor/factory is evaluating its business partner's security by in person visits, it may want to consider leveraging other types of required visits. For example, cross train personnel that test for quality control to also conduct security verifications.

iv. Circumstances that may require the self-assessment to be updated more frequently include an increased threat level from a source country, changes in source location, new critical business partners (those that actually handle the cargo, provide security to a facility, etc.).

F. Document social compliance program to address goods are not produced with forced labor

i. Vendors/factories should have a documented social compliance program in place that, at a minimum, addresses how the company ensures goods imported into the United States were not mined, produced or manufactured, wholly or in part, with prohibited forms of labor, i.e., forced, imprisoned, indentured, or indentured child labor.

ii. Forced Labor is defined by the International Labor Organization's Convention No. 29 as all work or service exacted from any person under the menace of any penalty and for which the said person has not offered himself voluntarily.

IV. Cybersecurity

In today's digital world, cybersecurity is the key to safeguarding a company's most precious assets – intellectual property, customer information, financial and trade data, and employee records, among others. With increased connectivity to the internet comes the risk of a breach of a company's information systems. This threat pertains to businesses of all types and sizes. Measures to secure a company's information technology (IT) and data are of paramount importance, and the listed criteria provide a foundation for an overall cybersecurity program for Vendor/factories.

Key Definitions:

Cybersecurity – Cybersecurity is the activity or process that focuses on protecting computers, networks, programs, and data from unintended or unauthorized access, change or destruction. It is the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits taken.

Information Technology (IT) – Computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure, and exchange all forms of electronic data.

Vendor/Factory requirements:

A. Have written cybersecurity policies and/or procedures

i. Vendors/factories must have comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems. The written IT policy, at a minimum, must cover all of the individual Cybersecurity criteria.

ii. Vendors/factories are encouraged to follow cybersecurity protocols that are based on recognized industry frameworks/standards. The *National Institute of Standards and Technology (NIST) is one such organization that provides a Cybersecurity Framework (https://www.nist.gov/cyberframework) that offers voluntary guidance based upon existing standards, guidelines, and practices to help manage and reduce cybersecurity risks both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. The Framework complements an organization's risk management process and cybersecurity program. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

iii. *NIST is a non-regulatory federal agency under the Department of Commerce that promotes and maintains measurement standards, and it is the technology standards developer for the US federal government. Vendors/factories can use NIST as a reference to determine similar or equivalent cybersecurity standards.

B. Must install sufficient software/hardware protection

i. To defend Information Technology (IT) systems against common cybersecurity threats, a company must install sufficient software/hardware protection from malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewalls) in vendors/factories' computer systems. Vendors/factories must ensure that their security software is current and receives regular security updates. Vendors/factories must have policies and procedures to prevent attacks via social engineering. If a data breach occurs or other unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and/or data.

C. IT infrastructure must be tested regularly to detect and act on vulnerabilities

i. Vendors/factories utilizing network systems must regularly test the security of their IT infrastructure.

ii. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.

iii. A secure computer network is of paramount importance to a business and ensuring that it is protected requires testing on a regular basis. This can be done by scheduling vulnerability scans. Just like a security guard checks for open doors and windows at a business, a vulnerability scan (VS) identifies openings on your computers (open ports and IP addresses), their operating systems, and software through which a hacker could gain access to the company's IT system. The VS does this by comparing the results of its scan against a database of known vulnerabilities and produces a correction report for the business to act upon. There are many free and commercial versions of vulnerability scanners available.

iv. The frequency of the testing will depend on various factors to include the company's business model and level of risk. For example, they should run these tests whenever there are changes to a business's network infrastructure. However, cyber-attacks are increasing amongst all sizes of businesses, and this needs to be considered when designing a testing plan.

D. Control unauthorized access of IT systems/data

i. A 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. All violators must be subject to appropriate disciplinary actions.

E. Review cybersecurity policies and procedures annually

i. 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, implemented and monitored as soon as possible

F. Access restriction dependent on job description

i. 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. Computer and network access must be removed upon employee terminations.

G. Assign individual account access

i. Individuals with access to Information Technology (IT) systems must use individually assigned accounts. 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.

ii. To guard IT systems against infiltration, user access must be safeguarded by going through an authentication process. Complex login passwords or passphrases, biometric technologies, and electronic ID cards are three different types of authentication processes. Processes that use more than one measure are preferred. These are referred to as two-factor authentication (2FA) or multi-factor authentication (MFA). MFA is the most secure because it requires a user to present two or more pieces of evidence (credentials) to authenticate the person's identity during the log-on process.

iii. MFAs can assist in closing network intrusions exploited by weak passwords or stolen credentials. MFAs can assist in closing these attack vectors by requiring individuals to augment passwords or passphrases (something you know) with something you have, like a token, or one of your physical features - a biometric.

iv. If using passwords, they need to be complex. The National Institute of Standards and Technology's (NIST) NIST Special Publication 800-63B: Digital Identity Guidelines, includes password guidelines (https://pages.nist.gov/800-63-3/sp800-63b.html). It recommends the use of long, easy to remember passphrases instead of words with special characters. These longer passphrases (NIST recommends allowing up to 64 characters in length) are considered much harder to crack because they are made up of an easily memorized sentence or phrase.

H. Have secure remote connectivity technology

i. Vendors/factories 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. Vendor/factories must also have procedures designed to prevent remote access from unauthorized users.

ii. VPNs are not the only choice to protect remote access to a network. Multi- factor authentication (MFA) is another method. An example of a multi- factor authentication would be a token with a dynamic security code that the employee must type in to access the network.

I. Secure access via personal devices

i. If vendors/factories 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.

ii. Personal devices include storage media like CDs, DVDs, and USB flash drives. Care will be used if employees are allowed to connect their personal media to individual systems since these data storage devices may be infected with malware that could propagate using the company's network.

J. Data encryption and data back-ups required

i. Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format.

ii. Daily backups may be needed because of the effect that data loss may have on multiple personnel, if production or shared servers are compromised/lose data. Individual systems may require less frequent backups, depending on what type of information is involved. Media used to store backups should preferably be stored at a facility offsite. Devices used for backing up data should not be on the same network as the one used for production work. Backing up data to a cloud is acceptable as an "offsite" facility.

K. Protect sensitive information

i. 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.

ii. Some types of computer media are hard drives, removable drives, CD-ROM or CD-R discs, DVDs, or USB drives.

iii. The National Institute for Systems and Technology (NIST) has developed the Government's data media destruction standards. Vendor/factories may want to consult NIST standards for sanitation and destruction of IT equipment and media.

iv. Hard Drive Destruction: http://ewastesecurity.com/nist-800-88-hard-drive-destruction/

v. Media Sanitation: https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization

Focus Area #2: Transportation Security

Transportation Security Focus Area Requirements:

V. Conveyance and Instruments of International Traffic Security

Smuggling schemes often involve the modification of conveyances and Instruments of International Traffic (IIT), or the hiding of contraband inside IIT. This criteria category covers security measures designed to prevent, detect, and/or deter the altering of IIT structures or surreptitious entry into them, which could allow the introduction of unauthorized material or persons.

At the point of stuffing/loading, procedures need to be in place to inspect IIT and properly seal them. Cargo in transit or “at rest” is under less control, and is therefore more vulnerable to infiltration, which is why seal controls and methods to track cargo/conveyances in transit are key security criteria.

Breaches in supply chains occur most often during the transportation process; therefore, Vendor/factories must be vigilant that these key cargo criteria be upheld throughout their supply chains.

Key Definitions:

Instruments of International Traffic (ITT) – Containers, flatbeds, unit load devices (ULDs), lift vans, cargo vans, shipping tanks, bins, skids, pallets, caul boards, cores for textile fabrics, or other specialized containers arriving (loaded or empty) in use or to be used in the shipment of merchandise in international trade.

Pest Contamination - visible forms of animals, insects or other invertebrates (alive or dead, in any lifecycle stage, including egg casings or rafts), or any organic material of animal origin (including blood, bones, hair, flesh, secretions, excretions); viable or non-viable plants or plant products (including fruit, seeds, leaves, twigs, roots, bark); or other organic material, including fungi; or soil, or water; where such products are not the manifested cargo within instruments of international traffic (i.e. containers, unit load devices, etc.).

Vendor/Factory requirements:

A. Secure storage of containers or conveyances

i. Conveyances and Instruments of International Traffic (IIT) must be stored in a secure area to prevent unauthorized access, which could result in an alteration to the structure of an Instruments of International Traffic or (as applicable) allow the seal/doors to be compromised.

ii. The secure storage of conveyances and IIT (both empty and full) is important to guard against unauthorized access.

B. Have written procedures for both security and agricultural inspections.

i. Vendors/factories must conduct inspections of conveyances and Instruments of International Traffic to look for visible pests and serious structural deficiencies

ii. The prevention of pest contamination via conveyances and IIT is of paramount concern, so an agricultural component has been added to the security inspection process

iii. Prior to loading/stuffing/packing, all conveyances and empty Instruments of International Traffic must undergo CTPAT approved security and agricultural inspections to ensure their structures have not been modified to conceal contraband or have been contaminated with visible agricultural pests.

iv. If visible pest contamination is found during the conveyance/ Instruments of International Traffic inspection, washing/vacuuming must be carried out to remove such contamination. Documentation must be retained for one year to demonstrate compliance with these inspection requirements.

C. Conduct container and conveyance inspection

i. A seven-point inspection (see **Exhibit A**) must be conducted on all empty containers and unit load devices (ULDs), including Front Wall, Left Side, Right Side, Floor, Ceiling/Roof, Inside/Outside Doors, Outside/Undercarriage

ii. The inspection of all containers and empty Instruments of International Traffic should be recorded on a checklist. The following elements should be documented on the checklist:

- Container/Trailer/Instruments of International Traffic number;
- Date of inspection;
- Time of inspection;
- Name of employee conducting the inspection; and
- Specific areas of the Instruments of International Traffic that were inspected.

iii. All security inspections should be performed in an area of controlled access and, if available, monitored via a CCTV system.

D. Examine container locking mechanism to detect tampering

i. Conveyances and Instruments of International Traffic (as appropriate) must be equipped with external hardware that can reasonably withstand attempts to remove it. The door, handles, rods, hasps, rivets, brackets, and all other parts of a container's locking mechanism must be fully inspected to detect tampering and any hardware inconsistencies prior to the attachment of any sealing device.

ii. Consider using containers/trailers with tamper resistant hinges. Vendor/factories may also place protective plates or pins on at least two of the hinges of the doors and/or place adhesive seal/tape over at least one hinge on each side.

E. Management random checks of conveyances

i. Based on risk, management personnel should conduct random searches of conveyances after the transportation staff have conducted conveyance/Instruments of International Traffic inspections.

ii. The searches of the conveyance should be done periodically, with a higher frequency based on risk. The searches should be conducted at random without warning, so they will not become predictable. The inspections should be conducted at various locations where the conveyance is susceptible: the carrier yard, after the truck has been loaded, and en route to the foreign loading port.

F. Conveyance tracking from factory to nominated foreign port or third-party logistics consolidation facility

i. Vendors/factories should work with their transportation providers to track conveyances from origin to final destination point. Specific requirements for tracking, reporting, and sharing of data should be incorporated within terms of service agreements with service providers.

ii. Vendors/factories should know the average time required to transport product from their factory to nominated port or CFS location. Transport times outside of average should be tracked, documented and monitored to ensure cargo was not compromised.

iii. If a credible (or detected) threat to the security of a shipment or conveyance is discovered, the vendor/factory must alert (as soon as feasibly possible) any business partners in the supply chain that may be affected and any law enforcement agencies, as appropriate.

VI. Seal Security

The sealing of trailers and containers, to include continuous seal integrity, continues to be a crucial element of a secure supply chain. Seal security includes having a comprehensive written seal policy that addresses all aspects of seal security; using the correct seals per CTPAT requirements; properly placing a seal on a container and verifying that the seal has been affixed properly.

<u>Vendor/Factory requirements</u>

A. Must have detailed, written high security seal procedures

i. Vendors/factories must have detailed, written high security seal procedures that describe how seals are issued and controlled at the facility and during transit. Procedures must provide the steps to take if a seal is found to be altered, tampered with, or has the incorrect seal number to include documentation of the event, communication protocols to partners, and investigation of the incident. The findings from the investigation must be documented, and any corrective actions must be implemented as quickly as possible.

ii. These written procedures must be maintained at the local, operating level so that they are easily accessible. Procedures must be reviewed at least once a year and updated as necessary.

iii. Written seal controls must include the following elements:

1. Controlling Access to Seals:
   - Management of seals is restricted to authorized personnel.
   - Secure storage.

2. Inventory, Distribution, & Tracking (Seal Log):
   - Recording the receipt of new seals.
   - Issuance of seals recorded in log.
   - Track seals via the log.
   - Only trained, authorized personnel may affix seals to Instruments of International Traffic (IIT)

3. Controlling Seals in Transit:
   - When picking up sealed IIT (or after stopping) verify the seal is intact with no signs of tampering.
   - Confirm the seal number matches what is noted on the shipping documents.

4. Seals Broken in Transit:
   - If load examined--record replacement seal number.
   - The driver must immediately notify dispatch when a seal is broken, indicate who broke it, and provide the new seal number.
   - The carrier must immediately notify the shipper, broker, and importer of the seal change and the replacement seal number.
   - The shipper must note the replacement seal number in the seal log.

5. Seal Discrepancies:
   - Hold any seal discovered to be altered or tampered with to aid in the investigation.
   - Investigate the discrepancy; follow-up with corrective measures (if warranted).
   - As applicable, report compromised seals to Genesco and the appropriate foreign government to aid in the investigation.

B. Secure shipments immediately after loading with high security seals

i. All shipments that can be sealed must be secured immediately after loading/stuffing/packing by the responsible party (i.e. the shipper or packer acting on the shipper's behalf) with a high security seal that meets or exceeds the most current International Standardization Organization (ISO) 17712 standard for high security seals. Qualifying cable and bolt seals are both acceptable. All seals used must be securely and properly affixed to Instruments of International Traffic that are transporting CTPAT Members' cargo to/from the United States.

ii. The high security seal used must be placed on the Secure Cam position, if available, instead of the right door handle. The seal must be placed at the bottom of the center most vertical bar of the right container door. Alternatively, the seal could be placed on the center most/left hand locking handle on the right container door if the secure cam position is not available. If a bolt seal is being used, it is recommended that the bolt seal be placed with the barrel portion or insert facing upward with the barrel portion above the hasp. Please also see Section 3 for additional requirements on camera placement in sensitive loading areas.

C. Use ISO 17712 high security seals

i. Vendors/factories (that maintain seal inventories) must be able to document the high security seals they use either meet or exceed the most current ISO 17712 standard.

ii. Acceptable evidence of compliance is a copy of a laboratory testing certificate that demonstrates compliance with the ISO high security seal standard.

D. Audit seal inventory

i. If vendor/factory maintains an inventory of seals, company management or a security supervisor must conduct audits of seals that includes periodic inventory of stored seals and reconciliation against seal inventory logs and shipping documents. All audits must be documented.

ii. As part of the overall seal audit process, dock supervisors and/or warehouse managers must periodically verify seal numbers used on conveyances and Instruments of International Traffic.

E. View, Verify, Tug and Twist seals to ensure seal affixed properly

i. CTPAT's seal verification process must be followed to ensure all high security seals (bolt/cable) have been affixed properly to Instruments of International Traffic and are operating as designed. The procedure is known as the VVTT process:

V – View seal and container locking mechanisms; ensure they are OK;

V – Verify seal number against shipment documents for accuracy;

T – Tug on seal to make sure it is affixed properly;

T – Twist and turn the bolt seal to make sure its components do not unscrew, separate from one another, or any part of the seal becomes loose.

ii. When applying cable seals, they need to envelop the rectangular hardware base of the vertical bars in order to eliminate any upward or downward movement of the seal. Once the seal is applied, make sure that all slack has been removed from both sides of the cable. The VVTT process for cable seals needs to ensure the cables are taut. Once it has been properly applied, tug and pull the cable in order to determine if there is any cable slippage within the locking body.

VII. Procedural Security

Procedural Security encompasses many aspects of the import-export process, documentation, and cargo storage and handling requirements. Other vital procedural criteria pertain to reporting incidents and notification to pertinent law enforcement. Additionally, CTPAT often requires that procedures be written because it helps maintain a uniform process over time. Nevertheless, the amount of detail needed for these written procedures will depend upon various elements such as a company's business model or what is covered by the procedure.

CTPAT recognizes that technology used in supply chains continues to evolve. The terminology used throughout the criteria references written procedures, documents, and forms, but this does not mean these have to be paper based. Electronic documents, signatures, and other digital technologies are acceptable to meet these measures.

The Program is not designed to be a "one size fits all" model; each company must decide (based on its risk assessment) how to implement and maintain procedures. However, it is more effective to incorporate security processes within existing procedures rather than create a separate manual for security protocols. This creates a more sustainable structure and helps emphasize that supply chain security is everyone's responsibility.

Vendor/Factory requirements

A. Secure cargo for extended periods of time

i. When cargo is staged overnight, or for an extended period of time, measures must be taken to secure the cargo from unauthorized access.

B. Inspect cargo staging areas

i. Cargo staging areas, and the immediate surrounding areas, must be inspected on a regular basis to ensure these areas remain free of visible pest contamination.

ii. Genesco requires that empty container parking areas, cargo staging areas and container loading areas should be done on clean grounds void of birds, animals, insects, plants, fruits, fungi, soil, water including but not limited to feces, feathers, eggs, blood, bones, leaves, twigs, roots, barks, or seeds.

iii. Preventative measures such as the use of baits, traps, or other barriers can be used as necessary. Removal of weeds or reduction of overgrown vegetation may help in the elimination of pest habitat within staging areas.

C. Supervise container stuffing by security officer/manager

i. The loading/stuffing of cargo into containers/IIT should be supervised by security officer/manager or other designated personnel.

D. Document point of stuffing

i. As documented evidence of the properly installed seal, digital photographs should be taken at the point of stuffing. To the extent feasible, these images should be electronically forwarded to the destination for verification purposes, as requested by Genesco.

ii. Photographic evidence may include pictures taken at the point of stuffing to document evidence of the cargo markings, the loading process, the location where the seal was placed, and properly installed seal.

E. Provide accurate and legible information related to cargo

i. Procedures must be in place to ensure that all information used in the clearing of merchandise/cargo is legible, complete, accurate, protect against the exchange, loss, or introduction of erroneous information, and reported on time.

F. Storage and recordkeeping of paper documentation must be secure

i. If paper is used, forms and other import/export related documentation should be secured to prevent unauthorized use.

ii. Measures, such as using a locked filing cabinet, can be taken to secure the storage of unused forms, including manifests, to prevent unauthorized use of such documentation.

G. Vendor/factory must provide accurate cargo information to Genesco.

i. The shipper or its agent must ensure that bill of ladings (BOLs) and/or manifests accurately reflect the information provided to the carrier, and carriers must exercise due diligence to ensure these documents are accurate. BOLs and manifests must be filed with U.S. Customs and Border Protection (CBP) in a timely manner. BOL information filed with CBP must show the first foreign location/facility where the carrier takes possession of the cargo destined for the United States. The weight and piece count must be accurate.

ii. When picking up sealed Instruments of International Traffic, carriers may

iii. rely on the information provided in the shipper's shipping instructions.

iv. Requiring the seal number to be electronically printed on the bill of lading (BOL) or other export documents helps guard against changing the seal and altering the pertinent document(s) to match the new seal number.

v. If goods are examined in transit, by a foreign Customs authority, or by CBP. Once the seal is broken by the government, there needs to be a process to record the new seal number applied to the container after examination. In some cases, this may be handwritten.

H. Review documents or cargo for suspicious shipments

i. Personnel must review the information included in import/export documents to identify or recognize suspicious cargo shipments.

ii. Relevant personnel must be trained on how to identify information in shipping documents, such as manifests, that might indicate a suspicious shipment.

iii. As a resource and based on risk, vendor/factories should take into account those CTPAT Key Warning Indicators for Money Laundering and Terrorism Financing Activities most applicable to the functions that the and/or their business entity perform in the supply chain. https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat

iv. Highway carrier personnel must be trained to review manifests and other documents in order to identify or recognize suspicious cargo shipments such as:

- Originated from or destined to unusual locations;
- Paid by cash or a certified check;
- Using unusual routing methods;
- Exhibit unusual shipping/receiving practices;
- Provide vague, generalized, or a lack of information

I. Have written procedures for Incident reporting

i. Vendors/factories must have written procedures for reporting an incident to include a description of the facility's internal escalation process.

ii. A notification protocol must be in place to report any suspicious activities or security incidents that may affect the security of the vendor's/factories' supply chain.

iii. Notification procedures must include the accurate contact information that lists the name(s) and phone number(s) of personnel requiring notification, as well as for law enforcement agencies. Procedures must be periodically reviewed to ensure contact information is accurate.

iv. Examples of incidents warranting notification to CBP include (but are not limited to) the following:

- Discovery of tampering with a container/IIT or high security seal;
- Discovery of a hidden compartment in a conveyance or IIT;
- An unaccounted new seal has been applied to an IIT;
- Smuggling of contraband to include people; stowaways;

- Unauthorized entry into conveyances, locomotives, vessels, or aircraft
- carriers;
- Extortion, payments for protection, threats, and/or intimidation;
- Unauthorized use of a business entity identifier (i.e., Importer of Record (IOR) number, Standard Carrier Alpha Code (SCAC), etc.).

J. Have written procedures to identify unauthorized/unidentified persons

i. Procedures must be in place to identify, challenge, and address unauthorized/unidentified persons. Personnel must know the protocol to challenge an unknown/unauthorized person, how to respond to the situation, and be familiar with the procedure for removing an unauthorized individual from the premises.

K. Have mechanism to report security related issues

i. Vendors/factories should set up a mechanism to report security related issues anonymously. When an allegation is received, it should be investigated, and if applicable, corrective actions should be taken.

ii. Internal problems such as theft, fraud, and internal conspiracies may be reported more readily if the reporting party knows the concern may be reported anonymously.

iii. Vendors/factories can set up a hotline program or similar mechanism that allows people to remain anonymous if they fear reprisal for their actions. It is recommended that any report be kept as evidence to document that each reported item was investigated and that corrective actions were taken.

L. Address shortages, overages and other discrepancies

i. All shortages, overages, and other significant discrepancies or anomalies must be investigated and resolved, as appropriate.

M. Cargo reconciliation

i. Arriving cargo should be reconciled against information on the cargo manifest. Departing cargo should be verified against purchase or delivery orders.

N. Conduct Incident investigations

i. Vendors/factories must initiate their own internal investigations of any security-related incidents (terrorism, narcotics, stowaways, absconders, etc.) immediately after becoming aware of the incident. The company investigation must not impede/interfere with any investigation conducted by a government law enforcement agency. The internal company investigation must be documented, completed as soon as feasibly possible, and made available to Genesco and any other law enforcement agency, as appropriate, upon request.

VIII. Agricultural Security

Agriculture is the largest industry and employment sector in the United States, an industry threatened by 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. Eliminating contaminants in all conveyances and all types of cargo may decrease CBP cargo holds, delays and commodity returns or treatments. Ensuring compliance with CTPAT's agricultural requirements will also help protect a key industry in the United States and the overall global food supply.

Key Definition:

Pest contamination – Visible forms of animals, insects or other invertebrates (alive or dead, in any lifecycle stage, including egg casings or rafts), or any organic material of animal origin (including blood, bones, hair, flesh, secretions, excretions); viable or non-viable plants or plant products (including fruit, seeds, leaves, twigs, roots, bark); or other organic material, including fungi; or soil, or water; where such products are not the manifested cargo within instruments of international traffic (i.e. containers, unit load devices, etc.).

Vendor/Factory requirements

A. Documented pest contamination procedures

i. Vendors/factories must have written procedures designed to prevent visible pest contamination to include compliance with Wood Packaging Materials (WPM) regulations. Visible pest prevention measures must be adhered to throughout the supply chain. Measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15).

ii. Genesco, in partnership with its freight forwarding partners, prohibits the use of wood packing materials.

Focus Area #3: People and Physical Security

People and Physical Security Focus Area Requirements:

IX. Physical Access Controls

Access controls prevent unauthorized access into facilities/areas, help maintain control of employees and visitors, and protect company assets. Access controls include the positive identification of all employees, visitors, service providers, and vendors at all points of entry.

Vendor/Factory requirements

A. Cargo handling

i. All cargo handling and storage facilities, including trailer yards and offices must have physical barriers and/or deterrents that prevent unauthorized access.

B. Entrance / Gate management

i. Gates where vehicles and/or personnel enter or exit (as well as other points of egress) must be manned or monitored. Individuals and vehicles may be subject to search in accordance with local and labor laws.

ii. It is recommended that the number of gates be kept to the minimum necessary for proper access and safety. Other points of egress would be entrances to facilities that are not gated.

C. Private passenger vehicles management

i. Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas, and conveyances.

ii. In order to minimize the risk of cargo being stolen or compromised by allowing for contraband commingled with cargo to have an easier pathway in/out, locate parking areas outside of fenced and/or operational areas - or at least at substantial distances from cargo handling and storage areas.

D. Lighting requirements

i. Adequate lighting must be provided inside and outside the facility including, as appropriate, the following areas: entrances and exits, cargo handling and storage areas, fence lines, and parking areas.

ii. Automatic timers or light sensors that automatically turn on appropriate security lights are useful additions to lighting apparatus.

E. Usage of security technology

i. Security technology should be utilized to monitor premises and prevent unauthorized access to sensitive areas.

ii. Security technology used to secure sensitive areas/access points includes alarms, access control devices, and video surveillance systems such as Closed Caption Television Cameras (CCTVs). Sensitive areas, as appropriate, may include cargo handling and storage areas, shipping/receiving areas where import documents are kept, IT servers, yards and storage areas for containers, areas where containers are inspected, and seal storage areas.

F. Policies on security technology

i. Vendors/factories who rely on security technology for physical security must have written policies and procedures governing the use, maintenance, and protection of this technology.

ii. At a minimum, these policies and procedures must stipulate:

- How access to the locations where the technology is controlled/managed or where its hardware (control panels, video recording units, etc.) is kept, is limited to authorized personnel;
- The procedures that have been implemented to test/inspect the technology on a regular basis;
- That the inspections include verifications that all of the equipment is working properly, and if applicable, that the equipment is positioned correctly;
- That the results of the inspections and performance testing is documented;
- That if corrective actions are necessary, these are to be implemented as soon as possible and that the corrective actions taken are documented;
- That the documented results of these inspections be maintained for a sufficient time for audit purposes.

iii. If a third-party central monitoring station (off-site) is utilized, the vendor/factory must have written procedures stipulating critical systems functionality and authentication protocols such as (but not limited to) security code changes, adding or subtracting authorized personnel, password revisions(s), and systems access or denial(s).

iv. Security technology policies and procedures must be reviewed and updated annually, or more frequently, as risk or circumstances dictate.

v. Security technology needs to be tested on a regular basis to ensure it is working properly. There are general guidelines to follow:

- Test security systems after any service work and during and after major repairs, modifications, or additions to a building or facility. A system's component may have been compromised, either intentionally or unintentionally.
- Test security systems after any major changes to phone or internet
- services. Anything that might affect the system's ability to communicate
- with the monitoring center deserves to be doublechecked.
- Make sure video settings have been set up properly: motion activated recording; motion detection alerts; images per second (IPS), and quality level.
- Make sure camera lenses (or domes that protect the cameras) are clean and lenses are focused. Visibility should not be limited by obstacles or bright lights.
- Test to make sure security cameras are positioned correctly and remain in the proper position (cameras may have been deliberately or accidentally moved).

G. Secure unauthorized access of all security technology

i. All security technology infrastructure must be physically secured from unauthorized access.

ii. Security technology infrastructure includes computers, security software, electronic control panels, video surveillance or closed-circuit television cameras, power and hard drive components for cameras, as well as recordings.

H. Camera system deployment requirements

i. Factories should utilize camera systems to monitor a facility's premises and sensitive areas to deter unauthorized access. Alarms should be used to alert a company to unauthorized access into sensitive areas.

ii. Sensitive areas, as appropriate, may include cargo handling and storage areas, shipping/receiving areas where import documents are kept, IT servers, yards and storage areas for containers areas where IIT are inspected, and seal storage areas.

iii. Cameras should be positioned to cover key areas of facilities that pertain to the import/export process.

iv. Cameras should be programmed to record at the highest picture quality setting reasonably available and be set to record on a 24/7 basis.

v. Based on risk, key sensitive areas may be monitored via security cameras. Positioning cameras correctly is important to enable the cameras to record as much of the physical "chain of custody" within the facility's control as possible.

vi. Specific areas of security focus would include cargo handling and storage; shipping/receiving; cargo loading process, sealing process; conveyance arrival/exit; IT servers; container inspections (security and agricultural); seal storage; and any other areas that pertain to securing international shipments.

vii. Cameras should have an alarm/notification feature, which would signal a "failure to operate/record" condition.

viii. A failure of video surveillance systems could be the result of someone disabling the system in order to breach a supply chain without leaving video evidence of the crime. The failure to operate feature can result in an electronic notification sent to predesignated person(s) notifying them that the device requires immediate attention.

ix. Periodic and random reviews, minimum of every 3-6 months, of the camera footage must be conducted (by management, security, or other designated personnel) to verify that cargo security procedures are being properly followed in accordance with law. Results of the reviews must be summarized in writing to include any corrective actions taken. The results must be maintained for a sufficient time for audit purposes.

x. Camera footage is only reviewed for cause (as part of an investigation following a security breach etc.), the full benefit of having cameras is not being realized. They are not only investigative tools; if used proactively, they may help prevent a security breach from occurring in the first place.

xi. Focus the random review of the footage on the physical chain of custody to ensure the shipment remained secure and all security protocols were followed. Some examples of processes that may be reviewed are the following:

- Cargo handling activities;
- Container inspections;
- The loading process;
- Sealing process;
- Conveyance arrival/exit; and
- Cargo departure, etc.

Purpose of the Review:

The review(s) is to evaluate overall adherence and effectiveness of established security processes, identify gaps or perceived weaknesses, and prescribe corrective actions in support of improvement to security processes. Based on risk (previous incidents or an anonymous report on an employee failing to follow security protocols at the loading dock, etc.), the Vendor/factories may target a review periodically.

Items to include in the written summary:

- The date of the review;
- Date of the footage that was reviewed;
- Which camera/area was the recording from;
- Brief description of any findings; and
- If warranted corrective actions.

I. Camera recording management

i. Camera recordings of footage covering key import/export processes should be maintained for a sufficient time for a monitored shipment to allow an investigation to be completed

ii. If a breach were to happen, an investigation would need to be conducted, and maintaining any camera footage that covered the packing (for export) and loading/sealing processes would be of paramount importance in discovering where the supply chain may have been compromised.

iii. Camera footage should be kept for 3 months from purchase order ship cancel date to destination market.

J. Have written procedures on granting, changing or removing ID badges and access to company devices

i. Vendor/factory must have written procedures governing how identification badges and access devices are granted, changed, and removed.

ii. Where applicable, a personnel identification system must be in place for positive identification and access control purposes. Access to sensitive areas must be restricted based on job description or assigned duties.

iii. Removal of access devices must take place upon the employee's separation from the company.

iv. Access devices include employee identification badges, visitor and vendor temporary badges, biometric identification systems, proximity key cards, codes, and keys. When employees are separated from a company, the use of exit checklists help ensure that all access devices have been returned and/or deactivated. For smaller companies, where personnel know each other, no identification system is required. Generally, for a company with more than 50 employees, an identification system is required.

K. Requirements for visitor, vendor or service provider access

i. Visitors, vendors, and service providers must present photo identification upon arrival, and a log must be maintained that records the details of the visit. All visitors should be escorted. In addition, all visitors and service providers should be issued temporary identification. If temporary identification is used, it must be visibly displayed at all times during the visit.

The registration log must include the following:

- Date of the visit;
- Visitor's name;
- Verification of photo identification (type verified such as license or national ID card). Frequent, well known visitors such as regular vendors may forego the photo identification, but must still be logged in and out of the facility;
- Time of arrival;
- Company point of contact; and
- Time of departure.

L. Have driver ID verification process

i. Drivers delivering or receiving cargo must be positively identified before cargo is received or released. Drivers must present government-issued photo identification to the facility employee granting access to verify their identity. If presenting a government-issued photo identification is not feasible, the facility employee may accept a recognizable form of photo identification issued by the highway carrier company that employs the driver picking up the load.

M. Driver / Cargo pick-up logs and procedures

i. A cargo pickup log must be kept to register drivers and record the details of their conveyances when picking up cargo. When drivers arrive to pick up cargo at a facility, a facility employee must register them in the cargo pickup log. Upon departure, drivers must be logged out. The cargo log must be kept secured, and drivers must not be allowed access to it.

The cargo pickup log should have the following items recorded:

- Driver's name;
- Date and time of arrival;
- Employer;
- Truck number;
- Trailer number;
- Time of departure;
- The seal number affixed to the shipment at the time of departure.

ii. A visitor log may double as a cargo log as long as the extra information is recorded in it.

iii. Prior to arrival, the carrier should notify the facility of the estimated time of arrival for the scheduled pick up, the name of the driver, and truck number. Where operationally feasible, vendor/factories should allow deliveries and pickups by appointment only.

iv. This criterion will help shippers and carriers to avoid fictitious pickups. Fictitious pick-ups are criminal schemes that result in the theft of cargo by deception that includes truck drivers using fake IDs and/or fictitious businesses set up for the purpose of cargo theft.

v. When a carrier has regular drivers that pick-up goods from a certain facility, a good practice is for the facility to maintain a list of the drivers with their pictures. Therefore, if it is not feasible to let the company know which driver is coming, the company will still be able to verify that the driver is approved to pick up cargo from the facility.

N. Scan arriving packages

i. Arriving packages and mail should be periodically screened for contraband before being admitted.

ii. Examples of such contraband include, but are not limited to, explosives, illegal drugs, and currency.

O. Delivery of goods can only be done in a specific monitored area

i. Delivery of goods to the consignee or other persons accepting delivery of cargo at the partner's facility should be limited to a specific monitored area.

P. Have specific written policies and procedures suited for the role of security guards

i. Security guard hold a very important role within a factory. Specific and appropriate work instructions for security guards must be contained in written policies and procedures. Management must periodically verify compliance and appropriateness with these procedures through audits and policy reviews.

X. Personnel Security

A company's human resource force is one of its most critical assets, but it may also be one of its weakest security links. The criteria in this category focus on issues such as employee screening and pre-employment verifications.

Many security breaches are caused by internal conspiracies, which is where one or more employees collude to circumvent security procedures aimed at allowing an infiltration of the supply chain. Therefore, vendor/factories must exercise due diligence to verify that employees filling sensitive positions are reliable and trustworthy. Sensitive positions include staff working directly with cargo or its documentation, as well as personnel involved in controlling access to sensitive areas or equipment. Such positions include, but are not limited to, shipping, receiving, mailroom personnel, drivers, dispatch, security guards, any individuals involved in load assignments, tracking of conveyances, and/or seal controls.

Vendor/Factory requirements

A. Verify employment history

i. Application information, such as employment history and references, must be verified prior to employment, to the extent possible and allowed under the law.

ii. In accordance with applicable legal limitations, and the availability of criminal record databases, employee background screenings should be conducted. Based on the sensitivity of the position, employee vetting requirements should extend to temporary workforce and contractors.

iii. Once employed, periodic reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.

iv. Employee background screening should include verification of the employee's identity and criminal history that encompass City, State, Provincial, and Country databases. Vendor/factories and their business partners should factor in the results of background checks, as permitted by local statutes, in making hiring decisions.

v. Background checks are not limited to verification of identity and criminal records. In areas of greater risk, it may warrant more in-depth investigations.

B. Employee Code of Conduct required and signed by employee

i. Vendors/factories must have an Employee Code of Conduct that includes expectations and defines acceptable behaviors. Penalties and disciplinary procedures must be included in the Code of Conduct. Employees/contractors must acknowledge that they have read and understood the Code of Conduct by signing it, and this acknowledgement must be kept in the employee's file for documentation.

ii. A Code of Conduct helps protect your business and informs employees of expectations. Its purpose is to develop and maintain a standard of conduct that is acceptable to the company. It helps companies develop a professional image and establish a strong ethical culture. Even a small company needs to have a Code of Conduct; however, it does not need to be elaborate in design or contain complex information.

XI. Education, Training and Awareness

CTPAT's security criteria are designed to form the basis of a layered security system. If one layer of security is overcome, another layer should prevent a security breach, or alert a company to a breach. Implementing and maintaining a layered security program needs the active participation and support of several departments and various personnel.

One of the key aspects to maintaining a security program is training. Educating employees on what the threats are and how their role is important in protecting the company's supply chain is a significant aspect to the success and endurance of a supply chain security program. Moreover, when employees understand why security procedures are in place, they are much more likely to adhere to them.

Vendor/Factory requirements

A. Establish security training and awareness program

i. Vendor/factories must establish and maintain a security training and awareness program to recognize and foster awareness of the security vulnerabilities to facilities, conveyances, and cargo at each point in the supply chain, which could be exploited by terrorists or contraband smugglers. The training program must be comprehensive and cover all of CTPAT's security requirements. Personnel in sensitive positions must receive additional specialized training geared toward the responsibilities that the position holds.

ii. One of the key aspects of a security program is training. Employees who understand why security measures are in place are more likely to adhere to them. Security training must be provided to employees, as required based on their functions and position, on a regular basis, and newly hired employees must receive this training as part of their orientation/job skills training.

iii. Training topics may include protecting access controls, recognizing internal conspiracies, and reporting procedures for suspicious activities and security incidents. When possible, specialized training should include a hands-on demonstration. If a hands-on demonstration is conducted, the instructor should allow time for the students to demonstrate the process.

iv. For CTPAT purposes, sensitive positions include staff working directly with import/export cargo or its documentation, as well as personnel involved in controlling access to sensitive areas or equipment. Such positions include, but are not limited to, shipping, receiving, mailroom personnel, drivers, dispatch, security guards, any individuals involved in load assignments, tracking of conveyances, and/or seal controls.

v. Vendors/factories must retain evidence of training such as training logs, sign in sheets (roster), or electronic training records. Training records should include the date of the training, names of attendees, and the topics of the training.

B. Targeted training for drivers and other personnel that conduct security inspections

i. Drivers and other personnel that conduct security and agricultural inspections of empty conveyances and containers must be trained to inspect their conveyances/IIT for both security and agricultural purposes.

ii. Refresher training must be conducted periodically, as needed after an incident or security breach, or when there are changes to company procedures.

Inspection training must include the following topics:

- Signs of hidden compartments;
- Concealed contraband in naturally occurring compartments; and
- Signs of pest contamination.

C. Validating training protocols

i. Vendors/factories should have measures in place to verify that the training provided met all training objectives.

ii. Understanding the training and being able to use that training in one's position (for sensitive employees) is of paramount importance. Exams or quizzes, a simulation exercise/drill, or regular audits of procedures etc. are some of the measures that the Vendor/factories may implement to determine the effectiveness of the training.

D. Conduct Trade Based Money Laundering and Terrorism Financing Training

i. Specialized training should be provided annually to personnel who may be able to identify the warning indicators of Trade Based Money Laundering and Terrorism Financing.

ii. Examples of personnel to receive such training include those responsible for trade compliance, security, procurement, finance, shipping, and receiving. Vendor/factories may take into account the CTPAT Warning Indicators for Trade Based Money Laundering and Terrorism Financing Activities document which will be provided as a module in the CTPAT training.

E. Targeted training on pest contamination

i. Training must be provided to applicable personnel on preventing visible pest contamination. Training must encompass pest prevention measures, regulatory requirements applicable to wood packaging materials (WPM), and identification of infested wood.

F. Targeted training on cybersecurity policies and procedures

i. As applicable based on their functions and/or positions, personnel must be trained on the company's cybersecurity policies and procedures. This must include the need for employees to protect passwords/passphrases and computer access.

ii. Quality training is important to lessen vulnerability to cyberattacks. A robust cybersecurity training program is usually one that is delivered to applicable personnel in a formal setting rather than simply through emails or memos.

G. Targeted training on operating and managing security technology systems

i. Personnel operating and managing security technology systems must have received training in their operation and maintenance. Prior experience with similar systems is acceptable. Self-training via operational manuals and other methods is acceptable.

H. Targeted training on security incident and suspicious activity reporting

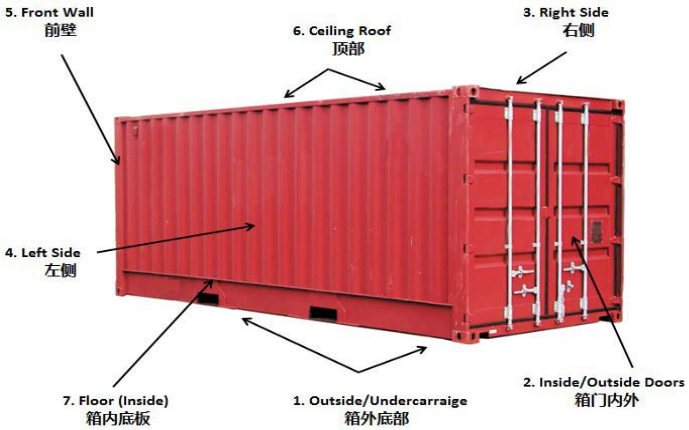
i. Personnel must be trained on how to report security incidents and suspicious activities.

ii. Procedures to report security incidents or suspicious activity are extremely important aspects of a security program, and training on how to report an incident can be included in the overall security training. Specialized training modules (based on job duties) may have more detailed training on reporting procedures to include specifics on the process - what to report, to whom, how to report it, and what to do next, after the report. CTPAT training that will be provided for Vendor/factories will include a module on reporting procedures.

Exhibit A

Seven-Point Container Inspection

Date of Inspection: ____________________



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.

Container Number: ____________________________ Full Name: ____________________________________

Seal Number: __________________________________ Signature: _____________________________________