ACE®

The helpful place.

Supplier CTPAT Compliance Handbook

May 2021

The helpful place.

Table of Contents

CTPAT Supply Chain Security Program

Customs Trade Partnership Against Terrorism (CTPAT)

Ace Hardware Corporation (AHC) participates in an important supply chain security program known as Customs Trade Partnership Against Terrorism (CTPAT) in partnership with U.S. Customs and Border Protection (CBP) to better secure its supply chain from contraband and terrorist infiltration. The CTPAT program was deployed in November 2001 joining public and private sector business partners in the fight against terrorism. Today, the CTPAT program has more than 11,500 members ranging from 3PL's, Highway Carriers, Customs Brokers, Importers, Rail Carriers, Consolidator and more whom work mutually to secure global supply chains.

The benefits of the CTPAT program to Ace's suppliers are:

a) Enhanced reputation (continued business with Ace Hardware Corporation)

b) Quicker movement of goods through U.S. Customs (reduced border times and faster payment to suppliers)

c) Improved security levels at factory location(s)

d) Improved understanding of U.S. Customs requirements for supply chains

For more CTPAT information visit the following links:

- https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat
- https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat-customs-trade-partnership-against-terrorism/apply/security-criteria

ACE
The helpful place.

Letter of Support

August 1, 2020

Customs Trade Partnership Against Terrorism
Ace Hardware Corporation / Statement of Support

Since 2006, Ace Hardware Corporation has been a proud Tier III member of the Customs Trade Partnership Against Terrorism (CTPAT). Ace began its CTPAT journey in November 2001. We communicate throughout the organization that CTPAT is a voluntary public-private initiative focused on relationships that strengthen our overall supply chain and border security. We understand it is voluntary but approach it as necessary to further protect our supply chain.

Customs and Border Protection (CBP) requests that businesses ensure the integrity of their security practices and communicate their security guidelines to their business partners throughout the supply chain. CTPAT offers businesses an opportunity to play a major role in the war against terrorism, drug trafficking, human smuggling, and illegal contraband thereby ensuring a more secure supply chain for their employees, suppliers, and customers. We have accepted that opportunity year over year.

Ace Hardware Corporation, its executives, management, and other key stakeholders, commit to participate in the CTPAT program, abiding to its procedures, and practices consistent with the CTPAT Minimum Security Criteria (MSC) enforced by Customs and Border Protection (CBP). As partners in the CTPAT program, it is the policy, procedure or practice of the Ace Hardware Corporation to:

- Implement and maintain policies, procedures and practices that are consistent with the CTPAT MSC.
- Review and update security policies, procedures and practices on a consistent basis. All Ace Hardware Corporation employees, contractors, service providers, and visitors are expected to comply with the CTPAT MSC policies and procedures as directed.
- Engage and cooperate with Customs / Border Protection (CBP) in its efforts to ensure the security of the supply chain.
- Meet the MSC requirements and security best practices.
- Assist in the global campaign to stop terrorism, drug trafficking, human smuggling and illegal contraband.
- Provide clear guidance and security direction including training for Ace Hardware Corporation employees, contractors, service providers, and others associated with the company.
- Consistently audit / evaluate internal and import partners to ensure conformance to CTPAT requirements.
- Investigate any situation or significant event which may be related to a breach in cargo security or any CTPAT criteria and notify the proper authorities.

Lori Bossmann

Lori Bossmann
EVP, Chief Supply Chain Officer

A Message to our Suppliers

Thank you for being our valued business partner! The purpose of this handbook is to help our suppliers understand the security requirements of the CTPAT Security Compliance Program that are expected of our business partners. Through mutual efforts, we can continue to protect Ace Hardware supply chains from risks of illegal contraband and terrorist activity.

Maintaining strong security controls from the factory level to point of delivery (USA) is critical to our mutual success. Therefore, please use this handbook, which outlines key security requirements of the CTPAT program, as guidance for security practice implementation.

We recommend that the information contained in this handbook be shared within your company to help ensure a thorough and complete understanding of CTPAT requirements, especially with team members who work directly with containers and cargo handling. Achieving a clear understanding of CTPAT security requirements will allow a smooth integration into your business processes.

Your support provides Ace Hardware not only with risk protection, but also enhances its brand and reputation by retaining its Tier III CTPAT Membership within the industry.

Business Conduct Guidelines

North Korean Forced Labor

Suppliers are prohibited from employing North Korean nationals or citizens for production of Ace Hardware goods. Suppliers are prohibited from engaging in any transaction that, in any way, involves a person or entity that is:

a. Located in North Korea; or
b. Controlled, directly or indirectly, by a North Korean person or entity; or
c. Involves a North Korean national or citizen.

China's Xinjiang Province

a. Vendors are prohibited from sourcing any components, materials, or products from China's Xinjiang Province that are sold to Ace Hardware.
b. Suppliers are prohibited from manufacturing any products from China's Xinjiang Province that are sold to Ace Hardware.

Components sourced from Sanctioned Countries

Ace Hardware will not accept *Product* that used components and/or raw materials from sanctioned countries in its production. Please visit the link below for additional information.

- https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/where-is-ofacs-country-list-what-countries-do-i-need-to-worry-about-in-terms-of-us-sanctions

Trafficking in Persons (Human Trafficking | Forced Labor)

Ace Hardware Corporation is committed to combatting the global crisis of human trafficking. All product suppliers, vendors, and other parties that furnish products or services to Ace Hardware should be committed to protect and advance human dignity rights in its global business practices and operations.

Ace has a long-standing zero-tolerance policy prohibiting trafficking related activities. As required by the Federal Acquisition Regulations (FAR 22.17), parties should not:

1. Engage in Trafficking in Persons;
2. Use forced labor, child labor, or indentured child labor, prison labor;
3. Procure commercial sex acts;

4. Destroy, conceal, confiscate, or otherwise deny access by an employee to the employee's identity or immigration documents, such as passports or drivers' licenses, regardless of issuing authority;
5. Use misleading or fraudulent practices during the recruitment of employees or offering of employment, such as failing to disclose, in a format and language accessible to the worker, basic information or making material misrepresentations during the recruitment of employees regarding the key terms and conditions of employment, including wages and fringe benefits, the location of work the living conditions, housing and associated costs (if employer or agent provided or arranged), any significant cost to be charged to the employee, and, if applicable, the hazardous nature of the work;
6. Use associated costs (if employer or agent provided or arranged), any significant cost to be charged to the employee, and, if applicable, the hazardous nature of the work;
7. Use misleading or fraudulent practices during the recruitment of employees or offering of employment, such as failing to disclose, in a format and language accessible to the worker, basic information or making material misrepresentations during the recruitment of employees regarding the key terms and conditions of employment, including wages and fringe benefits, the location of work, the living conditions, housing and associated costs (if employer or agent provided or arranged), any significant cost to be charged to the employee, and, if applicable, the hazardous nature of the work;
8. Use recruiters that do not comply with local labor laws of the country in which the recruiting takes place;
9. Charge employee's recruitment fees;
10. Fail to provide return transportation or pay for the cost of return transportation upon the end of employment for an employee who is not a national of the country in which the work is taking place and who was brought into that country for the purpose of working on a U.S. Government contract or subcontract (some limited exceptions apply);
11. Where housing is provided, provide or arrange housing that fails to meet the host country housing and safety standards; or
12. If required by law or contract, fail to provide an employment contract, recruitment agreement, or other required work document in writing.

Violation of the aforesaid could results in termination of the business relationship.

For more information, please visit the U.S. Federal Register via the link below:

- www.federalregister.gov search FAR 22.17; or
- https://www.federalregister.gov/documents/2018/12/20/2018-27541/federal-acquisition-regulation-combating-trafficking-in-persons-definition-of-recruitment-fees

Definitions

Trafficking in Persons is defined as:

1. The recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery; and
2. Sex trafficking in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such act has not attained 18 years of age.

Forced labor, Child labor, Indentured child labor are defined as:

- Forced labor is any work or service which people are forced to do against their will, under threat of punishment.

- Child forced labor refers to the exploitation of children through any form of work that deprives children of their childhood, interferes with their ability to attend regular school, and is mentally, physically, socially and morally harmful.

- Indentured child labor means all work from any person under the age of 18 under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily.

What you can do to help

If you become aware that Trafficking in Person is occurring, you may take any of the following actions to report the suspicious activity:

1. If you see or suspect unethical or illegal behavior, you may report your concerns anonymously by calling our toll-free hotline at **877-516-3384**; 24 hours a day, 7 days a week. You may call anytime from any location. You DO NOT have to give your name.

2. Anyone aware of potential human trafficking violations also may contact the Global Human Trafficking Hotline directly at **1-844-888-FREE** or help@befree.org .

3. Ace Hardware's policy and federal law prohibits retaliation against those who make reports of misconduct and prohibit interfering with employees' cooperation with government authority's investigation allegations.

Supplier Requirements for CTPAT

Ace Hardware Corporation requires that all suppliers develop and implement a written comprehensive plan for security procedures of their operations. The purpose of this is to create layers of protection that guard against the shipment of unauthorized materials such as, but not limited to drugs, biological agents, explosives, weapons, radioactive materials, human trafficking, human smuggling, or other illegal contraband from penetrating Ace Hardware's supply chains.

Ace Hardware will evaluate each supplier's security procedures during the factory audit process. The supplier must comply with all domestic laws, rules, and regulations governing contraband and must cooperate with all local, national, and foreign Customs agencies in protecting its business partners supply chains.

CTPAT Security Compliance Requirements

The **new** CTPAT Minimum Security Criteria (MSC) requirements, released in May 2019, takes a comprehensive approach towards supply chain security. New requirements to enhance the program impact the following areas:

a) **Cybersecurity** – To further secure IT systems and trade data that moves across cyberspace;
b) **Agricultural Security** – To protect the supply chain from pest and agricultural contaminants;
c) **Prevention of trade-based money laundering and terrorist financing**; and
d) Using **security technology** to strengthen existing physical security requirements.

MSC 3.0 - Business Partners

MSC-3.1	Suppliers should take a risk-based approach when sourcing raw materials from a 3rd party service provider. Suppliers should screen partners in areas of risk such as the use of force-labor/child labor/child indentured labor, money laundering, and terrorist funding. **Screening practice may include**: 1. Verifying the company's business address and length of time at that location 2. Learn about the company by researching it and its principles on the internet 3. Check business references 4. Requiring a security questionnaire to be completed yearly 5. Visit the location 6. Review U.S. Customs and Border Protection website – Withhold Release Order (WRO) for active detention orders issued: https://www.cbp.gov/trade/programs-administration/forced-labor/withhold-release-orders-and-findings

MSC-3.6	If weaknesses are identified during the Factory Audit process, Ace Hardware will allow a reasonable amount of time for the supplier to address and fix any issues identified. Ace's Quality team will follow-up to ensure deficiencies where strengthened. If an issue is rated as a serious risk, such as one that could threaten the security of a container, it should be addressed immediately.
MSC-3.7	Factory locations must pass a Factory audit in order to do business with Ace. Future factory audits are determined based on factory risk scores. As back-fill to Factory Audit time gaps, Ace now requires all factories to complete a CTPAT Security Questionnaire to ensure security measures outlined in this manual are practiced as expected. The results of the assessment will be used to help determine frequency of subsequent factory audits.
MSC-3.9	Suppliers should have a social compliance program documented that addresses how the facility ensures goods manufactured that are sold to the United States were not mined, produced, or manufactured, wholly or in part, with prohibited forms of labor, i.e., forced, imprisoned, child, or indentured child labor.

MSC 4.0 - Cybersecurity (Corporate Security)

CTPAT's Cybesecurity criteria serves to safeguarding intellectual property, customer information, financial and trade data, and employee records, among others.

Cybersecurity – Cybersecurity activites focuse on protecting computers, networks, programs, and data from 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.
Information Technology (IT) – IT includes computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure, and exchange all forms of electronic data.

MSC-4.1	Comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems must be maintained.
MSC-4.2	There must be enough software/ hardware protection from malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewalls) in computer systems. Suppliers must ensure that their security software is current and receives regular security updates. Policies and procedures to prevent attacks via social engineering must be in place. If a data breach occurs and data and/or equipment is lost, procedures must include a recovery plan.
MSC-4.3	If a network system is used, it must regularly test the security of the IT infrastructure. Corrective actions must be implemented as soon as possible for any vulnerability identified.
MSC-4.4	Cybersecurity policies should explain how information on cybersecurity threats is shared with their local government and other companies.
MSC-4.5	Suppliers must have a process in place that captures unauthorized access of IT systems/data or abuse of company policies and procedures, unauthorized access of internal systems or external websites, and tampering of business data by employees or contractors.
MSC-4.6	Cybersecurity policies and procedures must be reviewed and updated annually, or more frequently, if necessary.
MSC-4.7	Computer and network access must be restricted to job description or assigned duties and be removed upon employee separation.
MSC-4.8	Employees working with Information Technology (IT) systems must use individually assigned accounts. Each must use strong passwords, passphrases, etc. to protect from unauthorized access. User access to IT systems must be protected.

	Passwords and/or passphrases must be changed as soon as possible if there is evidence of or suspicions that it was compromised.
MSC-4.9	Locations that allow workers to remotely connect to a network must employ secure technologies, such as virtual private networks (VPNs) or Multi-factor Authentication (MFA), to allow employees to access the company's intranet securely. Procedures must be in place to prevent unauthorized access.
MSC-4.10	Personal devices used to conduct company work, must adhere to the company's cybersecurity policies and procedures. This should include regular security updates and a method to securely access the company's network. Examples of personal devices include storage media like CDs, DVDs, and USB flash drives.
MSC-4.11	Cybersecurity policies and procedures should address steps taken to prevent the use of counterfeit or improperly licensed technological equipment/product.
MSC-4.12	Data should be backed up regularly, daily or at least once a week. Sensitive and confidential data should be stored in an encrypted format. A second back-up 'off-site' is recommended.
MSC-4.13	Sensitive information stored on hardware, computer media, or other IT equipment related to import/export activities must be accounted for through regular inventories and properly destroyed when disposed of. Examples of computer media are hard drives, removable drives, CD-ROM or CD-R discs, DVDs, or USB drives.

MSC 5.0 - Conveyance and Instruments of International Traffic Security- (Transportation Security)

This section covers security measures designed to prevent, detect, and/or discourage the altering of container structures or entry into them to stop the introduction of unauthorized material or persons.

Instruments of International Traffic (ITT) – ITT includes any of the following used for international shipping: 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).

Pest contamination - Pests contamination includes any of the following that are visible to the human eye: 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.

MSC-5.1	Containers (both full and empty) must be stored in a secure area to prevent unauthorized access, which could result in the seal/container doors to be compromised.
MSC-5.2	Suppliers must have a written procedure for conducting both the 7-point container security inspection and pest/agricultural inspection.
MSC-5.3	**For Full Container Loads shipping factory direct –** Containers security and agricultural inspections must be conducted to ensure the container structure has not been modified to conceal contraband or have been contaminated with visible pest/agricultural contamination. **Inspection requirements for CTPAT shipments via ocean, air, and land borders (as applicable) by rail or intermodal freight:** A **7-Point Container Inspection** must be conducted on all empty containers: 1. Front wall; 2. Left side; 3. Right side; 4. Floor; 5. Ceiling/Roof; 6. Inside/outside doors, including the reliability of the locking mechanisms of the doors; and 7. Outside/Undercarriage.

	Mexico and Canada Only: Additional inspection requirements for land border crossings via highway carriers: Inspections of **conveyances and IIT** must be conducted at the point of loading/stuffing. These inspections must include 17-point inspections: **Tractors**: 1. Bumper/tires/rims; 2. Doors, tool compartments and locking mechanisms; 3. Battery box; 4. Air breather; 5. Fuel tanks; 6. Interior cab compartments/sleeper; and 7. Faring/roof. **Trailers**: 1. Fifth wheel area - check natural compartment/skid plate; 2. Exterior - front/sides; 3. Rear - bumper/doors; 4. Front wall; 5. Left side; 6. Right side; 7. Floor; 8. Ceiling/roof; 9. Inside/outside doors and locking mechanisms; and 10.Outside/Undercarriage.
MSC-5.4	Container inspection include fully inspecting the door, handles, rods, hasps, rivets, brackets, and all other parts of the container's locking mechanism to identify tampering and hardware inconsistencies. This must be done before affixing the high security bolt seal to the container.
MSC-5.5	A checklist should be used to document the inspection of all conveyances and empty Instruments of International Traffic. **The checklist should include the following data elements:** • 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. If the inspections are supervised, the supervisor should also sign the checklist. The container inspection checklist should be part of the shipping documentation packet.
MSC-5.6	Container inspections should be conducted in an area of controlled access and, if possible, under surveillance camera.
MSC-5.7	If pest\agricultural contamination is identified during the container inspection process, the container must be cleaned (vacuum, swept, or washed) to remove contaminants before loading freight onto the container. Dirty containers should not be used.
MSC-5.8	Managers should conduct random searches of containers after it has been loaded. This practice is used to identify any internal conspiracies. The searches should be conducted at random without warning, to keep them unpredictable.
MSC-5-15	Suppliers/shippers should have access to their land carriers GPS tracking system so that they can track the shipment.
MSC 5-29	Any suspicious activity or threats to the security of an Ace container should be immediately reported to Ace, law enforcement, and any other business partners that may be impacted.
OTHER	**See Appendix A to locate AHC's container, seal, and agricultural inspection sheet and instructions.** Suppliers are welcome to use their version of a 7-Point Container Inspection sheet if all CTPAT inspection data elements are included (include seal security, pest\agricultural inspections).

MSC 6.0 - Seal Security (Transportation Security) –

The Seal Security criteria addresses security seal requirements, such as using the correct seals, properly placing a seal on containers/trailers, verifying that seals are affixed properly, and evidence of documentation.
CTPAT approved seals: Seals that meet the current International Standardization Organization (ISO) 17712 standard for high security seals and qualifying cable and bolt seals.

MSC-6.1	***For Full Container Load shipments -*** Suppliers must have detailed, written high-security seal procedures for how seals are managed at their facility. Procedures should include a step-by-step plan of how situations are handled if a seal is identified to tampered with, appears altered, or the seal number sequence is disrupted. This process must be reviewed regularly (minimum one time per year). **Written seal controls must include the following elements -**

	Controlling Access to Seals: • Limit how seals are managed to authorized persons only • Provide a means for secure storage **Inventory, Distribution, & Tracking (Seal Log):** • Always record the receipt of new seals • Review how seals that are recorded on the seal log are assigned • Track seals via the log (try to identify number gaps or duplicate seal numbers) • Only trained and authorized employees should affix seals to containers • Confirm that the same seal number is reported on the shipping documents
MSC-6.2	Suppliers must seal all containers immediately after loading with a high security seal that meets or exceeds the current International Standardization Organization (ISO) 17712 standard for high security seals. All seals used must be properly affixed to containers and verified. **Affixing seal to container**: 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 (see Appendix B)**. 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. If the secure cam position is not available, the seal could be placed on the center most left-hand locking handle on the right container door. .
MSC-6.5	Suppliers that secure their own containers with a security seal, must document and have evidence that the high-security seals they use meets or exceeds the most current ISO 17712 standard. A copy of a laboratory testing certificate that demonstrates compliance with the ISO high-security seal standard serves as evidence. **Suppliers are expected to be aware of the tamper indicative features of the seals they purchase**.
MSC-6.6	***For suppliers who maintain inventory of seals –*** A seal audit that includes inventory of stored seals and reconciliation against seal inventory logs and shipping documents must be frequently conducted by management/security. **All audits must be documented.**
MSC-6.7	Suppliers who secure their own containers must follow CTPAT's seal verification process to ensure all high security seals (bolt/cable) have been affixed properly to containers. The procedure is known as the **V.V.T.T. process**: **Bolt seal VVTT check:** **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. **Cable seals:** If cable seals are used, 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. **Cable seal VVTT check:** For cable seals, ensure the cables are pulled tight. Once verified that it is properly affixed, tug and pull the cable to determine if the cables slip within the locking mechanism. As part of the overall seal audit process, dock supervisors and/or warehouse managers must periodically verify seal numbers used on containers.

Other	**See Appendix C** to locate CTPAT's Seal Verification and Inspection Process. Where possible, electronic photos should be taken of containers that capture (1) the container number, (2) seal number, (3) and the seal affixed to the container door.

MSC 7.0 - Procedural Security (Transportation Security)

The Procedural Security criteria encompasses many aspects of the import-export process, documentation, cargo storage and handling requirements, reporting incidents and notification to law enforcement. CTPAT requires that procedures be written because it helps maintain a uniform process over time.

MSC-7.1	Cargo must always be secure from unauthorized access, especially if it is staged overnight or for an extended period of time.
MSC-7.2	Facilities and cargo areas must be inspected to ensure they are free of pest and agricultural contamination.
MSC-7.4	A security officer/manager or other designated personnel should supervise the loading/stuffing of cargo into containers/trailers.
MSC-7.5	Digital photographs should be taken when the container/trailer is loaded to serve as documented evidence of a properly installed security seal. Photos may include pictures taken at the point-of-stuffing, the factory, and the location where the seal was placed. Photos should be available to Ace Hardware upon request.
MSC-7.6	All information reported on commercial documents should be legible, complete, accurate, protected against the exchange, loss, or introduction of erroneous information, and reported on time.
MSC-7.7	Suppliers who use paper import/export documentation, should ensure it is secured from unauthorized access. Paper documents should be kept in a locked filing cabinet.
MSC-7.8	The supplier, shipper, or its agent must ensure that information reported on the Bill of Lading (BOL) and/or manifests match the information provided to the carrier. Carriers must ensure that the weight and piece count reported on the documents is accurate. BOL information must show the first foreign location/facility where the carrier takes possession of the freight that is destined for the United States. Seal number are required to be electronically printed on the Bill of Lading (BOL) or other export documents to prevent the seal number and documents from being changed to match a new seal number.
MSC-7.23	Written procedures should be in place for reporting security incidents and should include the facility's internal escalation process. Procedures must be reviewed regularly to ensure contact information is accurate.
MSC-7.24	Procedures must be in place to identify, challenge, and address unauthorized/unidentified persons. If an unknown/unauthorized person is identified, team members must know how to respond to the situation and be familiar with the procedure for removing an unauthorized person from the premises.
MSC-7.25	Facilities should have a process in place that allows employees to report internal problems such as theft, fraud, and internal conspiracies, anonymously. Al claims should be investigated, and if applicable, corrective actions should be taken and documented.
MSC-7.27	Shortage and overages of product should be investigated.
MSC-7.28	Arriving cargo (raw materials) should be verified against the cargo manifest. Departing cargo should be verified against purchase or delivery orders.
MSC-7.29	Seal numbers should be reported to the consignee or its agent before the freight leaves the facility.
MSC-7.30	Seal numbers should be electronically printed on the bill of lading or other shipping documents.

MSC-7.37	All security related incidents within the facility must be investigated, corrected as quickly as possible, and documented.
Other	Conduct random, unannounced assessments of your company's security procedures on a routine basis to detect vulnerabilities and to verify the effectiveness of current security processes.

MSC 8.0 - Agricultural Security- New (Transportation Security)

The Agricultural Security criteria focuses on maintaining the supply chain free of agricultural and pest contamination. Eliminating contaminants in all containers may decrease CBP cargo holds, delays, avoid cost of fumigation treatments, shipment returns, and help protect the overall global food supply.

Pest contamination – For purposes of this manual, pest contamination is defined as *pests that are visible* to the human eye such as 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).

Pests related to WPM are those that *are not visible* to the human eye such as micro insects that live in wood.

Pests related to 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 are also included in the scope of "pest" contaminants.

Wood Packaging Materials (WPM) –

Wood or wood products (excluding paper products) used in supporting, protecting, or carrying a commodity. WPM includes items such as pallets, crates, boxes, reels, and dunnage.

MSC-8.1	Suppliers should have written procedures that explain actions taken to prevent visible pest contamination to include compliance with Wood Packaging Materials (WPM) regulations. Procedures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15). ISPM 15 requires all wood packaging material to be debarked and then heat treated or fumigated with methyl bromide and stamped or branded with the IPPC mark of compliance AKA the "**wheat stamp**". Products like paper, metal, plastic or wood panel products (i.e. oriented strand board, hardboard, and plywood) are exempt from ISPM 15 requirements.
Other	All containers and ITT should be clean and free from agricultural contaminants prior to loading. If agricultural contaminants are identified anywhere on the inside, outside, or undercarriage of the container, it must be thoroughly cleaned before loading to ensure contaminants are removed. **See Appendix A -** Container Inspection Sheet includes conducting the agricultural inspection. **See Appendix D -** Preventing the Spread of Invasive Pests Recommended Practices

MSC 9.0 - Physical Security (People and Physical Security)

The Physical Security criteria provides several deterrents/obstacles that will help prevent unwarranted access to cargo, sensitive equipment, and/or information.

MSC-9.1	Offices, cargo handling and storage facilities, and trailer yards must have security procedures in place to prevent unauthorized access.

MSC-9.2	**Perimeter fencing** should enclose cargo handling and storage areas. Fencing should be regularly inspected for integrity and damage by elected team members. High value goods should be stored in a fenced area under key and lock. Any signs of damage to the fence should be repairs quickly. Other acceptable barriers in place of perimeter fencing can be dividing wall, steep cliff, or dense thickets.
MSC-9.4	**Gates** where vehicles and/or team members enter or exit (as well as other points of entrance/access) must be staffed or monitored. Gates should be kept to the minimum necessary for safety and any other point of access that are not gated should be monitored.
MSC-9.5	**Employee parking – Team members** should be prohibited from parking in or adjacent to where freight is accessible such as the freight lot to reduce the risk of theft or other illegal activities.
MSC-9.6	All areas of the facility inside and outside must be well lit. Entrances, exits, cargo handling and storage areas, fence lines, and parking areas must all have adequate lighting.
MSC-9.7	**Security technology** such as surveillance cameras should be used to monitor access points and sensitive areas inside and the perimeter of the facility. • Sensitive areas are cargo handling and storage areas, shipping/receiving areas, where import documents are kept, IT servers, yard and storage areas where containers are kept and inspected, and areas were seals are stored.
MSC-9.8	***If applicable*** - Facilities that use security technology must have written policies and procedures that address the use, maintenance, and protection of this technology. These policies and procedures must specify: • That access to areas where technology is managed is limited to authorized employees; • The procedures that have been executed to test/review the technology regularly; • That the inspections verify that all the equipment is working as intended and positioned correctly to capture critical points of entry/exit/cargo handling areas; • That inspection and performance testing results are documented; • That corrective actions are documented and executed; • That the documented results of these inspections be kept long enough to review for purposes of an audit. If the facility contracts off-site monitoring (3rd party) to manage their security system, the facility must have written procedures specifying critical systems functionality and authentication protocols like security code changes, removing and adding authorized employees, password revisions, and systems access or denials. These policies and procedures must be reviewed and updated regularly. Security technology must be tested often to confirm it is working as designed. Following are guidelines to follow: • Test security systems if you've had service work or major repairs, modifications, or additions to a building or facility. These disruptions may compromise the security system, either intentionally or unintentionally. • Test security systems after any major changes to phone or internet services as this could affect how the systems communicate with the monitoring center. • Verify that video settings such as motion activated recording; motion triggers; images per second (IPS), and quality level, are set up correctly. • Verify that camera lenses are clean, and lenses are focused. • Test to make sure security cameras are positioned correctly and capturing critical areas of the facility and remain in the proper position especially after inclement weather.
MSC-9.9	Licensed/certified professionals should be used when installing security technology.

MSC-9.10	All security technology such as, computers, security software, electronic control panels, video surveillance or closed-circuit television cameras, power and hard drive components for cameras, as well as recordings, must be physically protected from unauthorized access.
MSC-9.11	Security technology systems should have an alternative power source such as an auxiliary power generation source or backup batteries that will allow the systems to keep operating if power is lost.
MSC-9.12	If cameras are used, cameras should monitor a facility's premises and sensitive areas to discourage unauthorized access. Alarms should be used to alert a facility of unauthorized access into sensitive areas such as cargo handling and storage areas, seal storage areas, shipping/receiving areas where import documents are kept, IT servers, yards and storage areas for containers and where containers are inspected.
MSC-9.13	If utilizing camera systems, they must be positioned to capture areas where import/export processes are executed. Cameras should record at the highest picture quality setting available and record 24/7. Key areas of process may include cargo handling and storage; shipping/receiving; the cargo loading process; the sealing process; seal storage; container arrival/exit; IT servers; 7-point container and seal inspections.
MSC-9.14	If utilizing camera systems, they should have a notification alert to communicate a "failure to operate/record" incident.
MSC-9.15	If utilizing camera systems, random and periodic reviews of the camera footage must be performed (by management, security) to verify that cargo security process are being followed. Corrective actions and documentation of the results must be maintained.
MSC-9.16	If cameras are being used, surveillance footage capturing key import/ export processes should be kept long enough to pull if an investigation was to commence.

MSC 10.0 - Physical Access Controls (People and Physical Security)

This section covers how to prevent unauthorized access into facilities/sensitive areas, how to preserve control of employees and visitor access, and protect company property and resources.

MSC-10.1	Written procedures regarding how identification badges and access devices are granted, changed, and removed should be maintained. If applicable, an employee ID system must be secured for positive identification and access control purposes. Access must be restricted to the employee's job description or assigned duties. The facility must collect access devices when the employee separates from the company. For smaller companies with less than 50 employees, and where employees know each other, an identification system is not required.
MSC-10.2	New/unfamiliar visitors and service providers must present photo identification when arriving to the facility, and a Visitors log must be maintained that records the details of the visit. An employee of the facility should complete the visitors log instead of the visitor to prevent false or incomplete reporting. All visitors and service providers should be provided temporary identification and escorted by an employee of the facility. Temporary identification must be visibly displayed during the visit. The Visitors 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). Well known visitors such as regular suppliers are not required to show photo identification but must still be logged in and out of the facility; • Time of arrival; • Company point of contact; and • Time of departure.
MSC-10.3	A positive ID check must be performed on all drivers picking up freight before cargo is released. Drivers must present photo identification to the facility employee such as a driver's license or a

	recognizable form of photo identification issued by the highway carrier company that employs the driver picking up the load.
MSC-10.4	A cargo pickup log must be used to document the driver ID information and the details of the load they are picking up. An employee of the facility (not the driver) must complete the cargo pickup log to avoid incorrect or incomplete reporting. Upon departure, drivers must be logged out. **Drivers must not be allowed access to the cargo pick-up log.** The following data points should be included on the log: • 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. **Note**: The visitor log may be used as a cargo log if all the information required for both logs is captured on it.
MSC-10.7	To avoid fictitious pick-ups, suppliers should schedule pick-ups by appointment only (if possible). Carriers picking up freight should notify the facility of the estimated pick-up time.
MSC-10.8	Mail and packages delivering to the facility for employee's should be periodically screened for contraband before being allowed in the facility. Examples of contraband include, but are not limited to, explosives, illegal drugs, and money.
MSC-10.10	For facilities that use security guards: Detailed work instructions for security guards must be clearly stated in written procedures and policies. Management must verify compliance of these procedures by conducting audits and by regularly reviewing/updating policies.

MSC 11.0 - Personnel Security (People and Physical Security)

The Personnel Security criteria focuses on issues related to employee screening and pre-employment verifications.

MSC-11.1	Suppliers must have written documented processes to screen new employees and to check existing employees. Application information, employment history and references, must be verified prior to employment, to the extent possible and allowed under the law. Labor and privacy laws in certain countries may not allow all the application information to be verified. However, due diligence is expected to verify application information when possible.
MSC-11.2	Within legal limitations, employee background screenings should be conducted. Based on the sensitivity of the position, employee vetting requirements should extend to temporary workforce and contractors. Once employed, periodic reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position. Employee background verification should include the person's identity, criminal history, city, state, provincial, and country. Results of background checks should be considered when making hiring decisions.
MSC-11.5	Suppliers should establish a Code of Conduct to clarify expectations and acceptable behaviors from employees. Penalties and disciplinary actions should be included in the Code of Conduct. An acknowledgement sheet should be signed and maintained.

MSC 12.0 - Education, Training, and Awareness (People and Physical Security)

The Education, Training, and Awareness criteria focuses on using education to teach employees about security risks, threats, and vulnerabilities and how their role in identifying these risks is important in protecting the company from a security incident.

MSC-12.1	Security training must be provided to employees based on their functions and position on a regular basis. New employees must receive this training as part of their orientation/job skills training. Evidence of training include 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. Training topics may include protecting access controls, recognizing internal conspiracies, and reporting procedures for suspicious activities and security incidents. Sensitive work roles include team members who work directly with import/export cargo or its documentation, team members involved in controlling access to sensitive areas. Examples of these positions include, but are not limited to, shipping, receiving, mailroom personnel, security guards, any individuals involved in load assignments, tracking of containers, and/or seal controls.
MSC-12.2	Employees that conduct security and agricultural inspections of empty must be trained to inspect their container for both security and pest/agricultural anomalies. Inspection training must include the following topics: • Signs of hidden compartments; • Concealed contraband in naturally occurring compartments; and • Signs of pest contamination.
MSC-12.4	Measures should be in place to verify that the training provided met all training objectives. Exams or quizzes, a simulation exercise/drill, or regular audits of procedures etc. are some of the measures that may be used to determine the effectiveness of the training.
MSC-12.8	Team members 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.
MSC-12.9	Team members that are operating and managing security technology systems must receive operations and maintenance training. Substitutes for training may include if team members have prior experience with similar systems or if they did self-training via operational manuals or other similar methods.
MSC-12.10	Team members must receive training on how to report security incidents and suspicious activities.
Other	An overall training session covering these topics is recommended to be provided yearly to existing employees and upon hire to new employees.

Appendix A

7-Point Container, Seal, and Agricultural Inspection Checklist

Prior to loading the container, supplier/warehouse must inspect and verify:

(1) The container structure is intact (e.g. no false walls, floors, or tampering evident in the physical structure)

(2) The locking mechanism of the doors are in good working order.

Date: _________________.

Supplier Name: _________________________________.

Container Number: __________________________________.

SEAL INSPECTION:

Seal Type:_______________| Seal#: ________________________| Seal condition: _________________.

Is the seal a High Security Seal? _____Yes _____No|

Is the seal affixed properly to the container? ___Yes _____No

Was the *V.V.T.T. inspection process performed? ____Yes _____No

Seal inspected by: ______________________________________Date _____________Time_________.

Instructions: Fill out the checklist by referring to the drawing and instructions provided on the next page.

Area of Inspection	Acceptable	If condition of the container is unacceptable, stop the inspection and notify a supervisor. Note irregularities below.
1. Outside/undercarriage condition *(Support beams should be visible)*	**___Y ___N**	
2. Inside and outside door condition *(Check locking mechanism for reliability.)*	**___Y ___N**	
3. Right side condition	**___Y ___N**	
4. Left side condition	**___Y ___N**	
5. Front wall Condition *(Make sure blocks and vents are visible)*	**___Y ___N**	
6. Ceiling / roof	**___Y ___N**	
7. Interior Floor condition	**___Y ___N**	
8. **Agriculture**: No seeds, pests, dirt in both interior and exterior, undercarriage of the container.	**___Y ___N**	

Inspection Tips

- Look for ***fake walls***
- Interior ***space of the container should match*** the length, height, and width reported on the papers
- Identify any ***bonding material,*** any ***different color points, bolts*** instead of rivets!

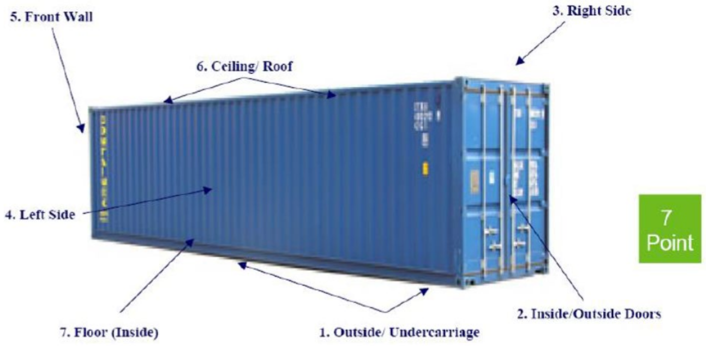
Container inspected by: ______________________________ Date: _____________Time:____________.

7-Point Trailer/Container Inspection Process

Inspect all trailers and containers before entering the facility. Please use the following checklist:

1. **Undercarriage:**
   a. Support beams should be visible
2. **Outside/Inside Doors:**
   a. Secure and reliable locking mechanisms
   b. Look for different color bonding material
   c. Check for Loose Bolts on locking hasp
   d. Check for added plates and repairs
3. **Right Side:**
   a. Unusual repairs to structural beams.
   b. Repairs to the walls on the inside of the container must be visible on the outside.
   c. Use tool to tap sidewalls. Listen & feel for hollow sound!
4. **Left Side:**
   a. Unusual repairs to structural beams.
   b. Repairs to the walls on the inside of the container must be visible on the outside.
   c. Use tool to tap sidewalls. Listen & feel for hollow sound!
5. **Front wall:**
   a. Be sure blocks and vents are visible.
   b. Use tool to tap front wall. Listen and feel for hollow sound!
   c. Use range finder, measuring tape and/or string to determine the length of container
6. **Ceiling/ Roof:**
   a. Ceiling is a certain height from floor. Be sure blocks & vents are visible.
   b. Do you experience an uncomfortable feeling inside the container? Do you sense that something is not right with the container?
   c. Repairs to the ceiling on the inside of the container should be visible on the outside.
   d. Use tool to tap ceiling. Listen for hollow sound. ◦
7. **Floor:**
   a. Floor should be a certain height from the ceiling
   b. Floor should be flat. Do not need to step up to get inside!
   c. Are there Different floor heights
   d. Are there unusual repairs

7-Point Container Inspection



Procedures should be in place to:

- Verify the physical integrity of the trailer structure prior to stuffing,
- Insure the reliability of the locking mechanisms of the doors.
- Border crossing tractors & trailers should be inspected upon arrival at the domestic facility.

Agriculture Inspection

The container must be free of pests, dirt, or any agricultural contamination. If contamination is identified on or in the container, either clean or return the container. Contaminated containers must not be used.

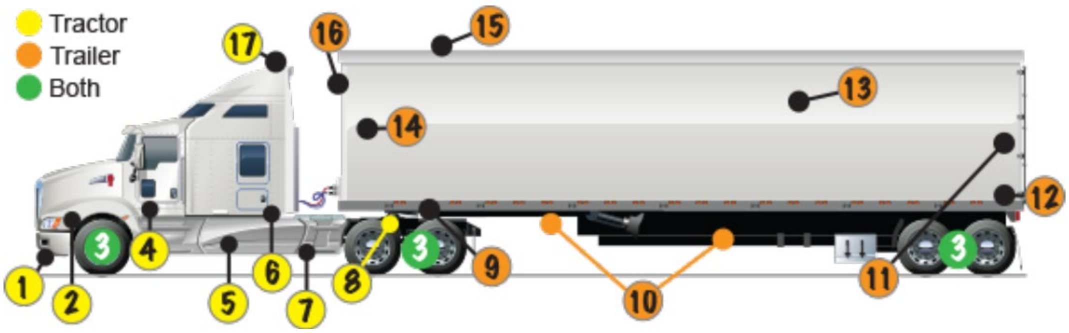
Wood Packaging Material (WPM)

Any solid wood packaging materials must follow the guidelines of USDA Wood Packing Materials (WPM) regarding treating and fumigating and contain proper treatment markings.

ACE
The helpful place.

CTPAT 17-Point Truck/Trailer Inspection Checklist

The 17-point inspection must be completed and documented on all containers/trailers/conveyances bound for the USA (Mexico and Canada). The trailer structure is intact, free from agricultural pests, seeds, dirt, and no false walls, floors, or signs of physical tampering.



1. **Bumper** ____________________
2. **Engine** ____________________
3. **Tires** ____________________
4. **Floor (truck)** ____________________
5. **Fuel tanks** ____________________
6. **Cab** ____________________
7. **Air tanks** ____________________
8. **Drive shaft** ____________________
9. **Fifth wheel** ____________________
10. **Outside/Undercarriage** ____________________
11. **Outside/Inside Doors** ____________________
12. **Floor (Trailer)** ____________________
13. **Side walls** ____________________
14. **Front wall** ____________________
15. **Ceiling/Roof** ____________________
16. **Refrigeration unit** ____________________
17. **Exhaust** ____________________

____
Printed name of person who conducted security inspection upon arrival

____
Signature and date

____
Date inspection was completed

____
Time inspection was completed

____
Printed name of person who conducted follow up security inspection

____
Signature and date

____
Seal # on container upon **arrival** at facility

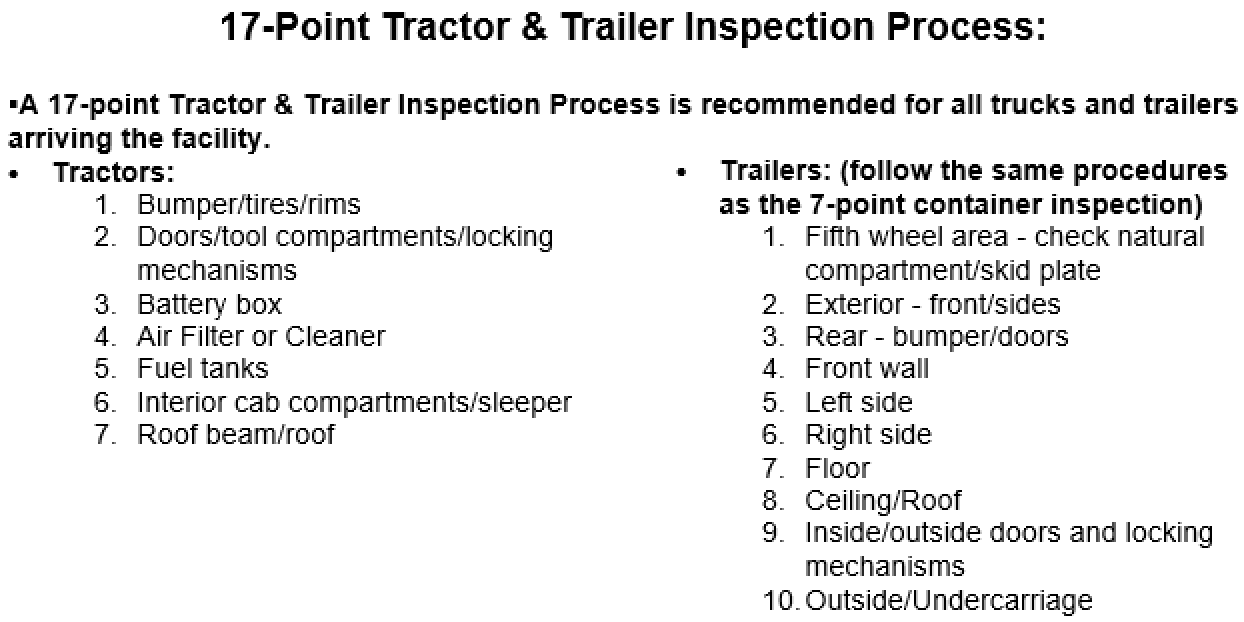
____
Seal # on container upon departure of facility

____
Printed name of person who **affixed** seal(s)

____
Signature and date

____
Printed name of person who **verified** physical integrity of seal(s)

____
Signature and date



17-Point Tractor & Trailer Inspection Process:

▪A 17-point Tractor & Trailer Inspection Process is recommended for all trucks and trailers arriving the facility.

- **Tractors:**
  1. Bumper/tires/rims
  2. Doors/tool compartments/locking mechanisms
  3. Battery box
  4. Air Filter or Cleaner
  5. Fuel tanks
  6. Interior cab compartments/sleeper
  7. Roof beam/roof

- **Trailers: (follow the same procedures as the 7-point container inspection)**
  1. Fifth wheel area - check natural compartment/skid plate
  2. Exterior - front/sides
  3. Rear - bumper/doors
  4. Front wall
  5. Left side
  6. Right side
  7. Floor
  8. Ceiling/Roof
  9. Inside/outside doors and locking mechanisms
  10. Outside/Undercarriage

Procedures should be in place to:

- Verify the physical integrity of the trailer structure prior to stuffing,
- Insure the reliability of the locking mechanisms of the doors.
- Border crossing tractors & trailers should be inspected upon arrival at the domestic facility.

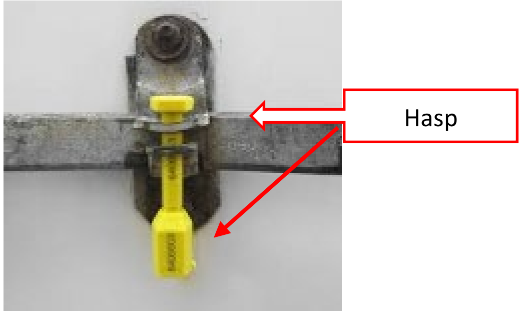
Agriculture Inspection: The container must be free of pests, dirt or any agricultural contamination. If contamination is identified on or in the container, either clean or return the container.

Wood Packaging Material (WPM): Any solid wood packaging materials must follow the guidelines of USDA Wood Packing Materials (WPM) regarding treating and fumigating.

Appendix B

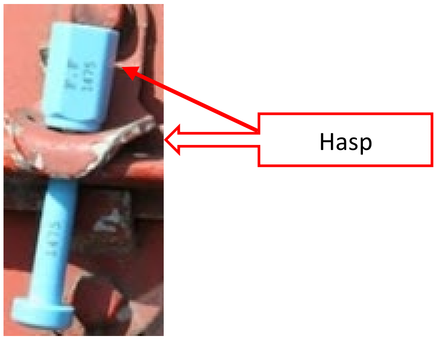
CTPAT Bolt-Seal Placement

Example 1: The standard method of affixing the bolt-seal to a container is by placing the barrel part of the seal **BELOW** the hasp.



Example 2: Ace Hardware containers should be secured using U.S. Customs (CBP) preferred method:

- Place the barrel part of the seal **ABOVE** the hasp.



Appendix C
CTPAT Seal Verification and Inspection Process (Origin)

A seal inspection process should be implemented throughout the supply chain. Only ISO Standard 17712 seals may be used on Ace Hardware containers.

V.V.T.T. - Use the V.V.T.T. Seal Inspection Process before opening a container/trailer.

- **V** – View seal & container locking mechanisms.
- **V** – Verify seal number for accuracy.
- **T** – Tug on seal to make sure it is affixed properly.
- **T** – Twist & Turn seal to make sure it does not unscrew.

View seal & container locking mechanisms.

- Excessive damage to the seal or locking mechanisms must be reported to a Supervisor before opening the container.

Verify seal number for accuracy.

- Compare with shipping documents and look for alterations to the seal numbers!

Tug on seal to make sure it is affixed properly.

- Seals that come apart must be reported to a Supervisor before opening the container. Human error might cause this to happen, or the container might have contraband inside.

Twist & Turn seal to make sure seal does not come off.

- Seals that are threaded, so they can be unscrewed are altered seals, and are reusable throughout the supply chain for multiple attacks. Notify supervisor Immediately.

CTPAT approved seals

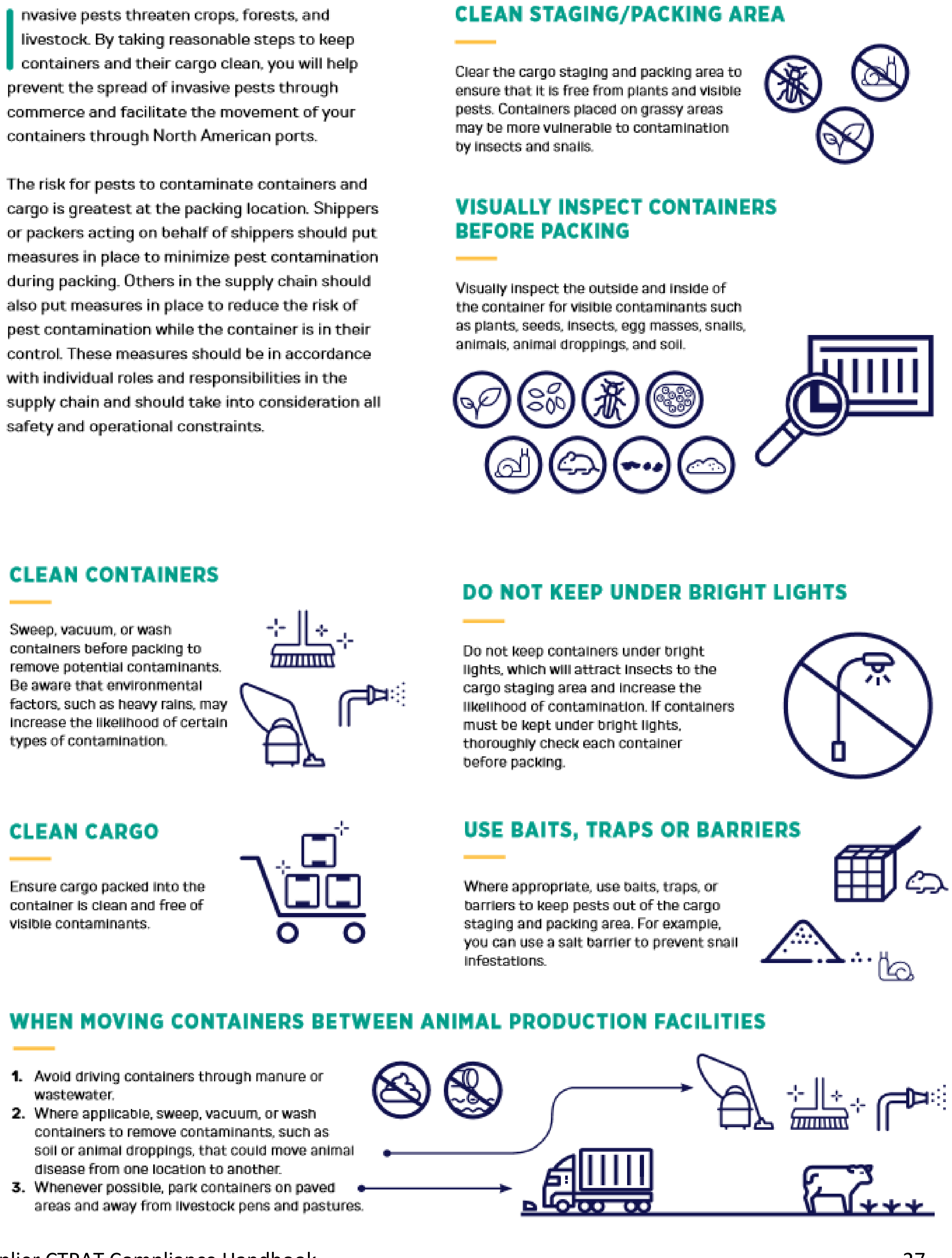
Only seals that meet the current International Standardization Organization (ISO) 17712 standard for high security seals and qualifying cable and bolt seals should be utilized to secure Ace Hardware containers.

Affixing seal to container

If a bolt seal is used, the bolt seal should be placed with the barrel portion or insert **facing upward with the barrel portion above the hasp**. The high-security seal used must be placed on the secure cam position, if possible, 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.

The helpful place.

Appendix D
Preventing the Spread of Invasive Pests Recommended Practices



Invasive pests threaten crops, forests, and livestock. By taking reasonable steps to keep containers and their cargo clean, you will help prevent the spread of invasive pests through commerce and facilitate the movement of your containers through North American ports.

The risk for pests to contaminate containers and cargo is greatest at the packing location. Shippers or packers acting on behalf of shippers should put measures in place to minimize pest contamination during packing. Others in the supply chain should also put measures in place to reduce the risk of pest contamination while the container is in their control. These measures should be in accordance with individual roles and responsibilities in the supply chain and should take into consideration all safety and operational constraints.

CLEAN STAGING/PACKING AREA

Clear the cargo staging and packing area to ensure that it is free from plants and visible pests. Containers placed on grassy areas may be more vulnerable to contamination by insects and snails.

VISUALLY INSPECT CONTAINERS BEFORE PACKING

Visually inspect the outside and inside of the container for visible contaminants such as plants, seeds, insects, egg masses, snails, animals, animal droppings, and soil.

CLEAN CONTAINERS

Sweep, vacuum, or wash containers before packing to remove potential contaminants. Be aware that environmental factors, such as heavy rains, may increase the likelihood of certain types of contamination.

DO NOT KEEP UNDER BRIGHT LIGHTS

Do not keep containers under bright lights, which will attract insects to the cargo staging area and increase the likelihood of contamination. If containers must be kept under bright lights, thoroughly check each container before packing.

CLEAN CARGO

Ensure cargo packed into the container is clean and free of visible contaminants.

USE BAITS, TRAPS OR BARRIERS

Where appropriate, use baits, traps, or barriers to keep pests out of the cargo staging and packing area. For example, you can use a salt barrier to prevent snail infestations.

WHEN MOVING CONTAINERS BETWEEN ANIMAL PRODUCTION FACILITIES

1. Avoid driving containers through manure or wastewater.
2. Where applicable, sweep, vacuum, or wash containers to remove contaminants, such as soil or animal droppings, that could move animal disease from one location to another.
3. Whenever possible, park containers on paved areas and away from livestock pens and pastures.

04/2019