Bloomberg Law®

Checklist

CTPAT Minimum Security Criteria Changes

Jennifer Diaz and Denise Calle,
Diaz Trade Law

CTPAT Minimum Security Criteria Changes

Contributed by Jennifer Diaz and Denise Calle, Diaz Trade Law

The following chart breaks down all major MSC changes by focus area, category, and I.D. The chart also includes criteria descriptions and implementation guidance, when applicable, for each category. The major changes arise when determining whether the criteria is a now a requirement ("must") or a suggestion ("should").

Focus Area: Corporate Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
Security Vision & Responsibility	1.3	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 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.	The goal of a review for CTPAT purposes is to ensure that its employees are following the company's security procedures. The review process does not have to be complex. The Member decides the scope of reviews and how in-depth they will be - based on its role in the supply chain, business model, level of risk, and variations between specific locations/sites. Smaller companies may create a very simple review methodology; whereas, a large multi-national conglomerate may need a more extensive process, and may need to consider various factors such as local legal requirements, etc. Some large companies may already have a staff of auditors that could be leveraged to help with security reviews. A Member may choose to use smaller targeted reviews directed at specific procedures. Specialized areas that are key to supply chain security such as inspections and seal controls may undergo reviews specific to those areas. However, it is useful to conduct an overall general review periodically to ensure that all areas of the security program are working as designed. If a Member is already conducting reviews as part of its annual review, that process could suffice to meet this criterion. For Members with high-risk supply chains (determined by their risk assessment), simulation or tabletop exercises may be included in the review program to ensure personnel will know how to react in the event of a real security incident.	MUST
Security Vision & Responsibility	1.4	The company's point(s) of contact (POC) to CTPAT must be knowledgeable about CTPAT program requirements. These individuals need to provide regular updates to upper management on issues related to the program, including the progress or outcomes of any audits, security	CTPAT expects the designated POC to be a proactive individual who engages and is responsive to his or her Supply Chain Security Specialist. Members may identify additional individuals who may help support this function by listing them as contacts in the CTPAT portal.	MUST

Focus Area: Corporate Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
		related exercises, and CTPAT validations.		
Risk Assessment	2.2	The international portion of the risk assessment should document or map the movement of the Member's cargo throughout its supply chain from the point of origin to the importer's distribution center. The mapping should include all business partners involved both directly and indirectly in the exportation/movement of the goods. As applicable, mapping should include documenting 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. Cargo is more vulnerable when "at rest," waiting to move to the next leg of its journey.	When developing a process to map supply chains, high risk areas are the first to be considered. When documenting the movement of all cargo, the Member is to 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). If any portion of the transport is subcontracted, this may also be considered because the more layers of indirect parties, the greater risk involved. The mapping exercise involves looking more in-depth at how your supply chain works. Besides identifying risks, it may also serve to find areas where a supply chain is inefficient, which may result in finding ways to decrease costs or lead times for receiving products.	SHOULD
Business Partners	3.1	CTPAT Members must have a written, risk based process for screening new business partners and for monitoring current partners. A factor that Members should include in this process is checks on activity related to money laundering and terrorist funding. To assist with this process, please consult CTPAT's Warning Indicators for Trade-Based Money Laundering and	The following are examples of some of the vetting elements that can help determine if a company is legitimate: • Verifying the company's business address and how long they have been at that address • Conducting research on the internet on both the company and its principals • Checking business references and • Requesting a credit report. 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	MUST

Focus Area: Corporate Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
		Terrorism Financing Activities.	chain and/or handle sensitive information/equipment are also included on the list to be screened, this includes brokers or contracted IT providers. How indepth to make the screening depends on the level of risk in the supply chain.	
Business Partners	3.5	When a CTPAT Member outsources or contracts elements of its supply chain, the Member must exercise due diligence (via visits, questionnaires, etc.) to ensure these business partners have security measures in place that meet or exceed CTPAT's Minimum Security Criteria (MSC).	Importers and exporters tend to outsource a large portion of their supply chain activities. Importers (and some exporters) are the parties in these transactions that usually have leverage over their business partners and can require that security measures are implemented throughout their supply chains, as warranted. For those business partners that are not CTPAT or accepted MRA Members, the CTPAT Member will exercise due diligence to ensure (when it has the leverage to do so) that these business partners meet the program's applicable security criteria. To verify adherence to security requirements, importers conduct security assessments of their business partners. The process to determine how much information is to be gathered regarding a business partner's security program is based on the Member's risk assessment, and if numerous supply chains, high-risk areas are the priority. 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 Member is sending a security questionnaire to its business partners, consider requiring the following items: • Name and title of the person(s) completing it • Date completed • Signature of the individual(s) who completed the document • *Signature of a senior company official, security supervisor, or authorized company representative to attest to the accuracy of the questionnaire • Provide enough detail in responses to determine compliance and • 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.	MUST

Focus Area: Corporate Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
			*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 (name and title are required).	
Business Partners	3.6	If weaknesses are identified during business partners' security assessments, they must be addressed as soon as possible, and corrections must be implemented in a timely manner. Members must confirm that deficiencies have been mitigated via documentary evidence.	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. 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. 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.	MUST
Business Partners	3.7	To ensure their business partners continue to comply with CTPAT's security criteria, Members should update their security assessments of their business partners on a regular basis, or as circumstances/risks dictate.	Periodically reviewing business partners' security assessments is important to ensure that a strong security program is still in place and operating properly. If a Member never required updates to its assessment of a business partner's security program, the Member would not know that a once viable program was no longer effective, thus putting the Member's supply chain at risk. Deciding on how often to review a partner's security assessment is based on the Member's risk assessment process. Higher risk supply chains would be expected to have more frequent reviews than low risk ones. If a Member 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. 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.).	SHOULD
Business Partners	3.9	CTPAT Members should have a documented social compliance program in place that, at	The private sector's efforts to protect workers' rights in their operations and supply chains can promote greater understanding of labor laws and standards and mitigate poor labor practices. These efforts also create an environment for	SHOULD

Focus Area: Corporate Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
		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.	better worker-employer relations and improve a company's bottom line. Section 307 of the Tariff Act of 1930 (19 U.S.C. § 1307) prohibits the importation of merchandise mined, produced or manufactured, wholly or in part, in any foreign country by forced or indentured child labor – including forced child labor. 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. A social compliance program is a set of policies and practices through which a company seeks to ensure maximum adherence to the elements of its code of conduct that cover social and labor issues. Social compliance refers to how a business addresses its responsibilities in protecting the environment, as well as the health, safety, and rights of its employees, the communities in which they operate, and the lives and communities of workers along their supply chains.	
Cyber Security	4.3	CTPAT Members using network systems must regularly test the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.	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. The frequency of the testing will depend on various factors including the company's business model and level of risk. For example, companies should run these tests whenever there are changes to a business's network infrastructure. However, cyber-attacks are increasing among all sizes of businesses, and this needs to be considered when designing a testing plan.	MUST
Cyber Security	4.12	Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format.	Data backups should take place as data loss may affect individuals within an organization differently. Daily backups are also recommended in case 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.	SHOULD

Focus Area: Corporate Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
Cyber Security	4.13	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.	Some types of computer media are hard drives, removable drives, CD-ROM or CD-R discs, DVDs, or USB drives. The National Institute for Systems and Technology (NIST) has developed the government's data media destruction standards. Members may want to consult NIST standards for sanitization and destruction of IT equipment and media. Media Sanitization: https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization	MUST

Focus Area: Transportation Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
Conveyance and Instruments of International Traffic Security	5.1	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 Instrument of International Traffic or (as applicable) allow the seal/doors to be compromised.	The secure storage of conveyances and Instruments of International Traffic (both empty and full) is important to guard against unauthorized access.	MUST
Conveyance and Instruments of International	5.2	The CTPAT inspection process must have written procedures for both security and agricultural inspections.	With the prevalence of smuggling schemes that involve the modification of conveyances or Instruments of International Traffic, it is imperative that Members conduct inspections of conveyances and Instruments of International Traffic to look for visible pests and serious structural deficiencies. Likewise,	MUST

Focus Area: Transportation Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
Traffic Security			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. Pest contamination is defined as 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.).	
Conveyance and Instruments of International Traffic Security	5.3	CTPAT Members must ensure that the following systematic CTPAT security and agricultural inspections are conducted. Requirements for these inspections will vary depending upon if the supply chain is land-based (Canada or Mexico) or if the supply chain originates overseas (ocean and air modes). Prior to stuffing/packing, all empty Instruments of International Traffic (IIT) must be inspected, and conveyances must also be inspected when they are crossing land borders into the United States. Inspection requirements for CTPAT shipments via ocean, air, and land borders (as applicable) by rail or intermodal freight: A seven-point inspection must be conducted on all empty containers and unit load devices (ULDs); and an eight-point inspection must be conducted on all empty	Security and agricultural inspections are conducted on instruments of international traffic (IIT) and conveyances to ensure their structures have not been modified to conceal contraband or have been contaminated with visible agricultural pests. Expectations for overseas supply chains are to inspect all instruments of IIT at the point of stuffing/packing. However, if an ocean/air based supply chain is higher risk, it may warrant including more extensive inspection procedures to include conveyances and/or inspections at marine port terminals or air logistics facilities. Usually, there are higher levels of risk involved in shipments with land border crossings, which is why both the conveyance and IIT undergo multiple inspections. Some examples of IIT for various modes are ocean containers, refrigerated containers/trailers, over-the-road trailers, flatbed trailers, tank containers, rail/boxcars, hoppers, and unit load devices (ULDs). The Public Library Section of the CTPAT Portal contains training material on security and agricultural conveyance/Instruments of International Traffic inspections.	MUST

Focus Area: Transportation Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
		refrigerated containers and ULDs: 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; 7. Outside/ Undercarriage; and 8. Fan housing on refrigerated containers. Additional inspection requirements for land border crossings via highway carriers: Inspections of conveyances and IIT must be conducted at conveyance/IIT storage yards. Where feasible, inspections must be conducted upon entering and departing the storage yards and at the point of loading/stuffing. These systematic inspections must include 17-point inspections: Tractors: 1. Bumper/tires/rims;		

Focus Area: Transportation Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
		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.		
Conveyance and Instruments of International Traffic Security	5.4	Conveyances and Instruments of International Traffic (as appropriate) must be equipped with external hardware that can reasonably withstand attempts to remove it.	Consider using containers/trailers with tamper resistant hinges. Members 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.	MUST

Focus Area: Transportation Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
		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.		
Conveyance and Instruments of International Traffic Security	5.29	If a credible (or detected) threat to the security of a shipment or conveyance is discovered, the Member 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.		MUST
Seal Security	6.2	All CTPAT 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 Organization for Standardization (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	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.	MUST

Focus Area: Transportation Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
		Members' cargo to/from the United States.		
Seal Security	6.6	If a Member maintains an inventory of seals, company management or a security supervisor must conduct a seal audit that includes periodic inventory of stored seals and reconciliation against seal inventory logs and shipping documents. All audits must be documented. 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.		MUST
Seal Security	6.7	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	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.	MUST

Focus Area: Transportation Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
		from one another, or any part of the seal becomes loose.		
Procedural Security	7.8	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.	When picking up sealed Instruments of International Traffic, carriers may rely on the information provided in the shipper's shipping instructions. Requiring the seal number to be electronically printed on the BOL or other export documents helps guard against changing the seal and altering the pertinent document(s) to match the new seal number. However, for certain supply chains, goods may be 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 IIT after examination. In some cases, this may be handwritten.	MUST
Procedural Security	7.37	Members 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		MUST

Focus Area: Transportation Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
		available to CBP/CTPAT and any other law enforcement agency, as appropriate, upon request.		

Focus Area: People and Physical Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
Physical Security	9.1	All cargo handling and storage facilities, including trailer yards and offices must have physical barriers and/or deterrents that prevent unauthorized access.		MUST
Physical Security	9.5	Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas, and conveyances.	Locate parking areas outside of fenced and/or operational areas - or at least at substantial distances from cargo handling and storage areas.	SHOULD
Physical Security	9.7	Security technology should be used to monitor premises and prevent unauthorized access to sensitive areas.	Electronic security technology used to secure/monitor sensitive areas and access points includes: burglary alarm systems (perimeter and interior) –these are also known as Intrusion Detection Systems (IDS); access control devices; and video surveillance systems (VSS) -including Closed Circuit Television Cameras (CCTVs). A CCTV/VSS system could include components such as Analog Cameras (coax-based), Internet Protocol-based (IP) cameras (network-based), recording devices, and video management software. Secure/sensitive areas, which would benefit from video surveillance, may include: cargo handling and storage areas, shipping/receiving areas where import documents are kept, IT servers, yard and storage areas for Instruments of International Traffic (IIT), areas where IIT are inspected, and seal storage areas.	SHOULD

Focus Area: People and Physical Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
Physical Security	9.8	Members who rely on security technology for physical security must have written policies and procedures governing the use, maintenance, and protection of this technology. At a minimum, these policies and procedures must stipulate: • That access to the locations where the technology is controlled or managed 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, they are to be implemented as soon as possible and the corrective actions are documented • That the documented results	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 should be double-checked. • Make sure video settings such as motion activated recording; motion detection alerts; images per second (IPS), and quality level, have been set up properly. • 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).	MUST

Focus Area: People and Physical Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
		of these inspections be maintained for a sufficient time for audit purposes. If a third party central monitoring station (off-site) is used, the CTPAT Member 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, and systems access or denials. Security technology policies and procedures must be reviewed and updated annually, or more frequently, as risk or circumstances dictate.		
Physical Security	9.13	If camera systems are deployed, cameras must be positioned to cover key areas of facilities that pertain to the import/export process. Cameras should be programmed to record at the highest picture quality setting reasonably available, and be set to record on a 24/7 basis.	Positioning cameras correctly is important to enable the cameras to record as much as possible of the physical "chain of custody" within the facility's control. Based on risk, key areas or processes may include cargo handling and storage; shipping/receiving; the cargo loading process; the sealing process; conveyance arrival/exit; IT servers; container inspections (security and agricultural); seal storage; and any other areas that pertain to securing international shipments.	MUST
Physical Security	9.14	If camera systems are deployed, cameras should have an alarm/notification	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	SHOULD

Focus Area: People and Physical Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
		feature, which would signal a "failure to operate/record" condition.	to predesignated person(s) notifying them that the device requires immediate attention.	
Physical Security	9.16	If cameras are being used, recordings of footage covering key import/export processes should be maintained on monitored shipments for a sufficient time to allow an investigation to be completed.	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. For monitoring, the CTPAT program recommends allotting at least 14 days after a shipment has arrived at its first point of distribution. This is where the container is first opened after clearing Customs.	SHOULD
Physical Access Controls	10.7	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, CTPAT Members should allow deliveries and pickups by appointment only.	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. 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.	SHOULD
Physical Access Controls	10.9	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.		SHOULD
Physical Access Controls	10.1	If security guards are used, 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.	Though guards may be employed at any facility, they are often employed at manufacturing sites, seaports, distribution centers, storage yards for Instruments of International Traffic, consolidator, and forwarders operating sites.	MUST

Focus Area: People and Physical Security				
Category	**I.D.**	**Criteria**	**Implementation Guidance**	**Must/ Should**
Personnel Security	11.1	Written processes must be in place to screen prospective employees and to periodically check current employees. Application information, such as employment history and references, must be verified prior to employment, to the extent possible and allowed under the law.	CTPAT is aware that labor and privacy laws in certain countries may not allow all of the application information to be verified. However, due diligence is expected to verify application information when permitted.	MUST
Personnel Security	11.5	CTPAT Members 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.	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.	MUST
Education, Training and Awareness	12.6	Specialized training should be provided annually to personnel who may be able to identify the CTPAT Warning Indicators of Trade-Based Money Laundering and Terrorism Financing.	Examples of personnel who should receive this training include those responsible for trade compliance, security, procurement, finance, shipping, and receiving. Members may take into account the CTPAT Warning Indicators for Trade-Based Money Laundering and Terrorism Financing Activities document.	MUST