Minimum Security Criteria – Air Carriers
November 2019

Note: Criteria ID numbers may not be sequential. ID numbers not listed are not applicable to Air Carriers.

First Focus Area: Corporate Security

1. Security Vision & Responsibility – For a CTPAT Member's supply chain security program

Implementation Guidance

			Must / Should
1.1	In promoting a culture of security, CTPAT Members should demonstrate their commitment to supply chain security and the CTPAT Program through a statement of support. The statement should be signed by a senior company official and displayed in appropriate company locations.	Statement of support should highlight the importance of protecting the supply chain from criminal activities such as drug trafficking, terrorism, human smuggling, and illegal contraband. Senior company officials who should support and sign the statement may include the president, CEO, general manager, or security director. Areas to display the statement of support include the company's website, on posters in key areas of the company (reception; packaging; warehouse; etc.), and/or be part of company security seminars, etc.	Should
1.2	To build a robust Supply Chain Security Program, a company should incorporate representatives from all of the relevant departments into a cross-functional team. These new security measures should be included in existing company procedures, which creates a more sustainable structure and emphasizes that supply chain security is everyone's responsibility.	Supply Chain Security has a much broader scope than traditional security programs. It is intertwined with Security, in many departments such as Human Resources, Information Technology, and Import/Export offices. Supply Chain Security programs built on a more traditional, security department-based model may be less	

ID	Criteria	Implementation Guidance	Must / Should
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 Terrorism Financing Activities.	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 chain and/or handle sensitive information/equipment are also included on the list to be screened; this includes brokers or contracted IT providers. How in-	

ID	Criteria	Implementation Guidance	Must / Should
3.4	The business partner screening process must take into account whether a partner is a CTPAT Member or a member in an approved Authorized Economic Operator (AEO) program with a Mutual Recognition Arrangement (MRA) with the United States (or an approved MRA). Certification in either CTPAT or an approved AEO is acceptable proof for meeting program requirements for business partners, and Members must obtain evidence of the certification and continue to monitor these business partners to ensure they maintain their certification.	Business partners' CTPAT certification may be ascertained via the CTPAT Portal's Status Verification Interface system. If the business partner certification is from a foreign AEO program under an MRA with the United States, the foreign AEO certification will include the security component. Members may visit the foreign Customs administration's website where the names of the AEOs of that Customs administration are listed, or request the certification directly from their business partners. Current United States MRAs include: New Zealand, Canada, Jordan, Japan, South Korea, the European Union (28 member states), Taiwan, Israel, Mexico, Singapore, the Dominican Republic, and Peru.	Must
3.5	When		

ID	Criteria	Implementation Guidance	Must / Should
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

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

   Key Definitions: Cybersecurity – Cybersecurity is the activity or process that focuses on protecting computers, networks, programs, and data from unintended or unauthorized access, change4 (s)6 (e)3 (cl)10 (da(f)-4tin)-4 (g)9 (ty)]TJ/TT0 1 Tfee4 (s)6 (e)3 (c)4.1 eityrneocusenfirk To

ID	Criteria	Implementation Guidance	Must / Should

ID	Criteria	Implementation Guidance	Must / Should
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 pEMC f Tw 3.4t hould be stord (n w)9.2 (ha)2died to son4.5 (ac)4.3 (ke)7 (c	

Second Focus Area: Transportation Security

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

ID	Criteria	Implementation Guidance	Must / Should
5.4	Conveyances and Instruments of International Traffic (as appropriate) must be equipped with external hardware that can reasonably withstand attempts to remove it. The door, handles, rods, hasps, rivets, brackets, and all other parts of a container's locking mechanism must be fully inspected to detect tampering and any hardware inconsistencies prior to the attachment of any sealing device.	Consider using containers/trailers with tamper resistant h679 (m)8	

ID	Criteria	Implementation Guidance	Must / Should
	companies approved for the effective disposal of these items. The following areas must be inspected for security reasons:		

ID	Criteria	Implementation Guidance	Must / Should
5.13	When an air carrier allows a Unit Load Device (ULD) to leave their control, written procedures must be in place to track the ULD and its		

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

ID	Criteria	Implementation Guidance	Must / Should
6.1	CTPAT Members must have detailed, written high-security seal procedures that describe how seals are issued and controlled at the facility and during o9t[(i)5.kesri(h)-8 (e)esal03 (r)(h103 (r))-8 (e)[(t)2w 9.96 -0 0 9.96 14[, wnTQq14 wri[(t)2. 9.96 -0 0 9.96 11-]TJ33C (r)4.6 (a)2 (ns)10.1 (t.3 ((bep6.4 (r).7)]T6 (t).d wq108.		

ID	Criteria	Implementation Guidance	Must / Should
	Seals Broken in Transit: • If a load is examined, record the replacement seal number. • The driver must immediately notify dispatch when a seal is broken, indicate who broke the seal, and provide the new seal number. • The carrier must immediately notify the shipper, broker, and importer of the seal change and the replacement seal number. • The shipper must note the replacement seal number in the seal log. **Seal Discrepancies:** • Retain altered or tampered seals to aid in investigations. • Investigate the discrepancy; follow-up with corrective measures (if warranted). • As applicable, report compromised seals to CBP and the appropriate foreign government to aid in the investigation.		
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 Members' cargo to/from the United States.	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

7.

ID	Criteria	Implementation Guidance	Must / Should
		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.	
7.23	CTPAT Members must have written procedures for reporting an incident, which includes a description of the facility's internal escalation process. A notification protocol must be in place to report any suspicious activities or security incidents (such as drug seizures, discovery of stowaways, etc.) that take place anywhere around the world and which affects the security of the member's supply chain. As applicable, the Member must report any global incidents to its Supply Chain Security Specialist, the closest port of entry, any pertinent law enforcement agencies, and business partners that may be part of the affected supply		

a c t , o ( ) 1 . 3 (9 (6 o) - 4 2 ((i)

8. **Agricultural Security –** Agriculture is the largest industry and employment sector in the U.S. It is also an industry threatened by the introduction of foreign animal and plant contaminants such as soil, manure, seeds, and plant and animal material which may harbor invasive and destructive pests and diseases. Eliminating contaminants in all conveyances and in all types of cargo may decrease CBP cargo holds, delays, and commodity returns.

Third Focus Area: People and Physical Security

9. <u>Physical Security</u> – Cargo handling and storage facilities, Instruments of International Traffic storage areas, and facilities where import/export documentation is prepared in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access.

One of the cornerstones of CTPAT is flexibility, and security programs should be customized to fit each company's circumstances. The need for physical security can vary greatly based on the Member's role in the supply chain, its business model, and level of risk. The physical security criteria provides a number of deterrents/obstacles that will help prevent unwarranted access to cargo, sensitive equipment, and/or information, and Members should employ these security measures throughout their supply chains.

ID	Criteria	Implementation Guidance	Must / Should
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
9.2	Perimeter fencing should enclose the areas around cargo handling and storage facilities. If a facility handles cargo, interior fencing should be used to secure cargo and cargo handling areas. Based on risk, additional interior fencing should segregate various types of cargo such as domestic, international, high value, and/or hazardous materials. Fencing should be regularly inspected for integrity and damage by designated personnel. If damage is found in the fencing, repairs should be made as soon as possible.	Other acceptable barriers may be used instead of fencing, such as a dividing wall or natural features that are impenetrable or, otherwise impede, access such as a steep cliff or dense thickets.	Should

ID	Criteria	Implementation Guidance	Must / Should
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
9.6	Adequate lighting must be provided inside and outside the facility including, as appropriate, the following areas: entrances and exits, cargo handling and storage areas, fence lines, and parking areas.	Automatic timers or light sensors that automatically turn on appropriate security lights are useful additions to lighting apparatus.	Must
9.7	Security technology should be utilized 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.	

ID	Criteria	Implementation Guidance	Must / Should
9.10			

ID	Criteria	Implementation Guidance	Must / Should
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. a c	Should

ID	Criteria	Implementation Guidance	Must / Should
10.2	Visitors, vendors, and service providers must present photo identification upon arrival, and a log must be maintained that records the details of the visit. All visitors should be escorted. In addition, all visitors and service providers should be issued temporary identification. If temporary identification is used, it must be visibly displayed at all times during the visit. The registration log must include the following: • Date of the visit; • Visitor's name; • Verification of photo identification (type verified such as license or national ID card). Frequent, well known visitors such as regular vendors may forego the photo identification, but must still be logged in and out of the facility; • Time of arrival; • Company point of contact; and • Time of departure.		Must
10.8	Arriving packages and mail should be periodically screened for contraband before being admitted.	Examples of such contraband include, but are not limited to, explosives, illegal drugs, and currency.	Should

ID	Criteria	Implementation Guidance	Must / Should
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

12. Education, Training and Awareness – CTPAT's security criteria are designed

ID	Criteria	Implementation Guidance	Must / Should
12.9	Personnel operatiati		