Minimum Security Criteria – U.S. Importers
November 2019

Note: Criteria ID numbers may not be sequential. ID numbers not listed are not applicable to U.S. Importers.

First Focus Area: Corporate Security

1. **Security Vision & Responsibility –** For a CTPAT Member's supply chain security program to become and remain effective, it must have the support of a company's upper management. Instilling security as an integral part of a company's culture and ensuring that it is a companywide priority is in large part the responsibility of the company's leadership.

ID	Criteria security and the CTPAT pro

ID	Criteria	Implementation Guidance	Must / Should

3. Business Partners – CTPAT Members engage with a variety of business partners, both domestically and internationally. For those business partners who directly handle cargo and/or import/export documentation, it is crucial for the Member to ensure that these business partners have appropriate security measures in place to secure the goods throughout the international supply chain. When business partners subcontract certain functions, an additional layer of complexity is added to the equation, which must be considered when conducting a risk analysis of a supply chain.

Key Definition: Business Partner – A business partner is any individual or company whose actions may affect the chain of custody security of goods being imported to or exported from the United States via a CTPAT Member's supply chain. A business partner may be any party that provides a service to fulfil a need within a company's international supply chain. These roles include all parties (both directly and indirectly) involved in the purchase, document preparation, facilitation, handling, storage, and/or movement of cargo for, or on behalf, of a CTPAT Importer or Exporter Member. Two examples of indirect partners are subcontracted carriers and overseas consolidation warehouses – arranged for by an agent/logistics provider.

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-depth to make the screening depends on the level of risk in the supply chain.	

CTPAT

ID	Criteria	Implementation Guidance	Must / Should
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	

ID	Criteria	Implementation Guidance	Must / Should
3.9	CTPAT Members should have a documented social compliance program in place that, at a minimum, addresses how the company ensures goods imported into the United States were not mined, produced or manufactured, wholly or in part, with prohibited forms of labor, i.e., forced, imprisoned, indentured, or indentured child labor.	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 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, chi2-0.9 (l)-1 (6 Tc (t)]T(ch)-4 3Td55ec)-2.7 n i229 Td( )T.7 (ur)4F3.4 8-7 (n)-9.14 (b)-9t cff Acto58 (	

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, change or destruction. It is the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits taken.

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

Td(0.376 e0 T3(h)p)10 (7)Tj4 2(5)-4 (d)]T7 (a)108 (n)-4 (d)-260(I 36 ref*22 Td( )TjEMC 14( )r)101(n avi5-4 (o)2610 4 2o

ID	Criteria	

ID	Criteria	Implementation Guidance	Must / Should
4.8	Individuals with access to Information Technology (IT) systems must use individually assigned accounts. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication, and user access to IT systems must be safeguarded. Passwords and/or passphrases must be changed as soon as possible if there is evidence of compromise or reasonable suspicion of a compromise exists.	To guard IT systems against infiltration, user access must be safeguarded by going through an authentication process. Complex login passwords or passphrases, biometric technologies, and electronic ID cards are three different types of authentication processes. Processes that use more than one measure are preferred. These are referred to as two-factor authentication (2FA) or multi-factor authentication (MFA). MFA is the most secure because it requires a user to present two or more pieces of evidence (credentials) to authenticate the person's identity during the log-on process. MFAs can assist in closing network intrusions exploited by weak	

ID	Criteria	Implementation Guidance	Must / Should

[redacted]	Implementation Guidance	Must / Should
[redacted]	ata backups should take place as data loss may affect individuals within n organization differently. Daily backups are also recommended in case roduction or shared servers are compromised/lose data. Individual ystems may require less frequent backups, depending on what type of nformation is involved. ledia used to store backups should preferably be stored at a facility ffsite. Devices used for backing up data should not be on the same etwork as the one used for production work. Backing up data to a cloud acceptable as an "offsite" facility.	Should
[redacted]	ome types of computer media are hard drives, removable drives, CD- [redacted]	Must

[redacted]

ID	Criteria	Implementation Guidance	Must / Should

ID	Criteria	Implementation Guidance	

ID	Criteria	Implementation Guidance	Must / Should
	Seals Broken in Transit: • If a load		

ID	Criteria	Implementation Guidance	Must / Should
6.5	CTPAT Members (that maintain seal inventories) must be able to document that the high-security seals they use meet or exceed the most current ISO 17712 standard.	Acceptable evidence of compliance is a copy of a laboratory testing certificate that demonstrates compliance with the ISO high-security seal standard. CTPAT Members are expected to be aware of the tamper indicative features of the seals they purchase.	Must
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
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 – Twi6 -0 0 9.9 (ur)4.6 (a)2.429.24 Tj0.hT8h 0 Td(5.9 (0 Td[w -26.71m94 Td(5.a1 (g)-3 Td(5.9(w -2a)-7.9 nb 1095(o)1.9 (c)-5.8 (e)9.1107.297.14 (i)-hi)5 (p397.14 (i.1 (3		

ID	Criteria	Implementation Guidance	Must / Should
7.6	Procedures must be in place to ensure that all information used in the clearing of merchandise/cargo is legible; complete; accurate; protected against the exchange, loss, or introduction of erroneous information; and reported on time.		Must
7.7	If paper documents are used, forms and other import/export related documentation should be secured to prevent unauthorized use.	Measures, such as using a locked filing cabinet, can be taken to secure the storage of unused forms, including manifests, to prevent unauthorized use of such documentation.	Should
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 mu		

ID	Criteria	Implementation Guidance	Must / Should
7.27	All shortages, overages, and other significant discrepancies or anomalies must be investigated and resolved, as appropriate.		Must
7.28	Arriving cargo should be reconciled against information on the cargo manifest. Departing cargo should be verified against purchase or delivery orders.		Should
7.29	Seal numbers assigned to specific shipments should be transmitted to the consignee prior to departure.		Should
7.30	Seal numbers should be electronically printed on the bill of lading or other shipping documents.		Should
7.37	Members must initiate their own internal investigations of any security-related incidents (terrorism, narcotics, stowaways, absconders, etc.)		

8. **<u>Agricultural Security</u> –** 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

Third Focus Area: People and Physical Security

9. **Physical Security –** 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
9.4	Gates where vehicles and/or personnel ente01 Tw 9.p-9.1 (el)-36 9.p		

ID	Criteria	Implementation Guidance	Must / Should
9.10	All security technology infrastructure must be physically secured from unauthorized access.	Security technology infrastructure includes computers, security software, electronic control panels, video surveillance or closed circuit television cameras, power and hard drive components for cameras, as well as recordings.	Must
9.11	Security technology systems should be configured with an		

ID	Criteria	Implementation Guidance	Must / Should
9.15	If camera systems are deployed, periodic, random reviews of the camera footage must be conducted (by management, security, or other designated personnel) to verify that cargo security procedures are being properly followed in accordance with the law. Results of the reviews must be summarized in writing to		

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;		

ID	Criteria	Implementation Guidance	Must / Should
10.4	A cargo pickup log must be kept to register drivers and record the details of their conveyances when picking up cargo. When drivers arrive to pick up cargo at a facility, a facility employee must register them in the cargo pickup log. Upon departure, drivers must be logged out. The cargo log must be kept secured, and drivers must not be allowed access to it. The cargo pickup log should ha-1.4 (go)-4.l it.		

ID	Criteria	Implementation Guidance	Must / Should
11.2	In accordance with applicable legal limitations, and the availability of criminal record databases, employee background screenings should be conducted. Based on the sensitivity of the position, employee vetting requirements should extend to temporary workforce and contractors. Once employed, periodic reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position. Employee background screening should include verification of the employee's identity and criminal history, encompassing city, state, provincial, and country databases. CTPAT Members and their business partners should factor in the results of background checks, as permitted by local statutes, in making hiring decisions. Background checks are not limited to verification of identity and criminal records. In areas of greater risk, it may warrant more in-depth investigations.		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. **<u>Education, Training and Awareness</u> –** CTPAT’s security criteria are designed to form the basis of a layered security system. If one layer of security is overcome, another layer should prevent a security breach, or alert a company to a breach. Implementing and maintaining a layered security program needs the active participation and support of several departments and various personnel.

ID	Criteria	Implementation Guidance	

ID	Criteria	Implementation Guidance	Must / Should
12.8	As applicable, based on their functions and/or positions, personnel must be trained on the company's cybersecurity policies and procedures. This must include the need for employees to protect passwords/passphrases and computer access.	Quality training is important to lessen vulnerability to cyberattacks. A robust cybersecurity training program is usually one that is delivered to applicable personnel in a formal setting rather than simply through emails or memos.	Must
12.9	Personnel operating and managing security technology systems must receive operations and maintenance training in their specific areas. Prior experience with similar systems is acceptable. Self-		