ID	Criteria	

2. **Risk Assessment –** The continuing threat of terrorist groups and criminal organizations targeting supply chains underscores the need for Members to assess existing and potential exposure to these evolving threats. CTPAT recognizes that when a company has multiple supply chains with numerous business partners, it faces greater complexity in securing those supply chains. When a company has numerous supply chains, it should focus on geographical areas/supply chains that have higher risk.

   When determining risk within their supply chains, Members must consider various factors such as the business model, geographic location of suppliers, and other aspects that may be unique to a specific supply chain.

   Key Definition: Risk – A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence. What determines the level of risk is how likely it is that a threat will happen.

ID	

ID	Criteria	Implementation Guidance	Must /

ID	Criteria	Implementation Guidance	Must / Should
		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 auaB	

ID	Criteria	Implementation Guidance	Must /

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

ID	Criteria	

ID	Criteria	Implementation Guidance	Must / Should
4.2	To defend Information Technology (IT) systems against		

ID	Criteria	Implementation Guidance	Must / Should
4.4	Cybersecurity policies should address how a Member shares information on cybersecurity threats with the government and other business partners.	Members are encouraged to share information on cybersecurity threats with the government and business partners within their supply chain. Information sharing is a key part of the Department of Homeland Security's mission to create shared situational awareness of malicious cyber activity. CTPAT Members may want to join the National Cybersecurity and Communications Integration Center (NCCIC - https://www.us-cert.gov/nccic). The NCCIC shares information among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations. Cyber and industrial control systems users can subscribe to information products, feeds, and services at no cost.	Should
4.5	A system must be in place to identify unauthorized access of IT systems/data or abuse of policies and procedures including improper access of internal systems or external websites and tampering or altering of business data by employees or contractors. All violators must be subject to appropriate disciplinary actions.		Must
4.6	Cybersecurity policies and procedures must be reviewed annually, or more frequently, as risk or circumstances dictate. Following the review, policies and procedures must be updated if necessary.	An example of a circumstance that would dictate a policy update sooner than annually is a cyber attack. Using the lessons learned from the attack would help strengthen a Member's cybersecurity policy.	Must
4.7	User access must be restricted based on job description or assigned duties. Authorized access must be reviewed on a regular basis to ensure access to sensitive systems is based on job requirements. Computer and network access must be removed upon employee separation.		Must

Second Focus Area: Transportation Security

5. **Conveyance and Instruments of International Traffic Security** – Smuggling schemes often involve the modification of conveyances and Instruments of International Traffic (IIT), or the hiding of contraband inside IIT. This criteria category covers securit

ID	Criteria	Implementation Guidance	Must / Should
5.6	All security inspections should be performed in an area of controlled access and, if available, monitored via a CCTV system.		Should
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

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 transit. Procedures must provide the steps to take if a seal is altered, tampered with, or has the incorrect seal number, including documentation of the event, communication protocols to partners, and investigation of the incident. The findings from the investigation must be documented, and any corrective actions must be implemented as quickly as possible. These written procedures must be maintained at the local operating level so that they are easily accessible. Procedures must be reviewed at least once a year and updated as necessary. Written seal controls must include the following elements:		Must

ID	Criteria	Implementation Guidance	Must / Should

ID	Criteria	Implementation Guidance	Must / Should
7.24	Procedures must be in place to identify, challenge, and address unauthorized/unidentified persons. Personnel must know the protocol to challenge an unknown/unauthorized person, how to respond to the situation, and be familiar with the procedure for removing an unauthorized individual from the premises.		Must
7.25	CTPAT Members should set up a mechanism to report security related issues anonymously. When an allegation is received, it should be investigated, and if applicable, corrective actions should be taken.	Internal problems such as theft, fraud, and internal	

ID	Criteria	Implementation Guidance	Must / Should
7.29	Seal numbers assigned to specific shipments should be transmitted to the consignee prior to departure.		Should
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,		

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 handliT6pC 113.4 351.84 281.64 12.24 ref*d( )TjET9.96 ET9.96		

ID	Criteria	Implementation Guidance	Must / Should

ID	Criteria	Implementation Guidance	Must / Should
	Cameras should be programmed to record at the highest picture quality setting reasonably available, and be set to record on a 24/7 basis.	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.	
9.14	If camera systems are deployed, cameras should have an alarm/notification feature, which would signal a "failure to operate/record" condition.	A failure of video surveillance systems could be the result of someone disabling the system in order to breach a supply chain without leaving video evidence of the crime. The failure to operate feature can result in an electronic notification sent to predesignated person(s) notifying them that the device requires immediate attention.	Should

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.	Should

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

ID	Criteria	Implementation Guidance	Must / Should
10.1	CTPAT Members must have written procedures governing how identification badges and access devices are granted, changed, and removed. Where applicable, a personnel identification system must be in plac18i9-ifor positive identification and acc18i9-ss controdes.urpo Access to sensitive areas must be restricted based on job description or asigned duties Removal of acces devices must take place when the employees separateifrom the company	Access devices include employee identification badges, visitor and vendor temporary badges, biometric identification systems proximity key cards, codes, and keys. When employees are separated from a company the use of exit checklists help ensure that all access devices have been returned and/or deactivated. For smaller companies, where personnel know each other, no identification system is required. Generally, for a company with more than 50 employees, an identification sytem is required.	

ID	Criteria	Implementation Guidance	Must / Should
10.2			

ID	Criteria	Implementation Guidance	Must / Should
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 u countries may not allow all of the application information to be verified. However, due diligence is expected to verify application information when permitted.	Must
11.2	In accordance with applicable legal limitations, and the availability of criminal record databases, employee background screenings should be conducted.		

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

ID	Criteria	Implementation Guidance	Must / Should
12.1	Members must establish and maintain a security training and awareness program to recognize and foster awareness of the security vulnerabilities to facilities, conveyances, and cargo at each point in the supply chain, which could be exploited by terrorists or contraband smugglers. The treronts mo5 (o)1.9 (Tc 0.00)]TJ0 -1.229 .6 (s)1pt.5 (.h(o)1.9 n)4.6 2(l)5 (e)9..6 (rv (ci8(ug)6.1 (1 (ni)5.1 ()]TJ0 -1.229 v3 (h2 (e)9.1 (d by 1 (ni)		

ID	Criteria	Implementation Guidance	Must / Should
12.4	CTPAT Members should have measures in place to verify that the training provided met all training objectives.	Understanding the training and being able to use that training in	