Minimum Security Criteria – U.S. Importers
March 2020

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	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 viable over the long run because the responsibility to carry out the security measures are concentrated among fewer employees, and, as a result, may be susceptible to the loss of key personnel.	Should

ID	Criteria	Implementation Guidance	Must / Should
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
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 related exercises, and CTPAT validations.	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

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. A high probability of an occurrence will usually equate to a high level of risk. Risk may not be eliminated, but it can be mitigated by managing it – lowering the vulnerability or the overall impact on the business.

ID	Criteria	Implementation Guidance	Must / Should
2.1	CTPAT Members must conduct and document the amount of risk in their supply chains. CTPAT Members must conduct an overall risk assessment (RA) to identify where security vulnerabilities may exist. The RA must identify threats, assess risks, and incorporate sustainable measures to mitigate vulnerabilities. The Member must take into account CTPAT requirements specific to the Member's role in the supply chain.	The overall risk assessment (RA) is made up of two key parts. The first part is a self-assessment of the Member's supply chain security practices, procedures, and policies within the facilities that it controls to verify its adherence to CTPAT's minimum-security criteria, and an overall management review of how it is managing risk. The second part of the RA is the international risk assessment. This portion of the RA includes the identification of geographical threat(s) based on the Member's business model and role in the supply chain. When looking at the possible impact of each threat on the security of the Member's supply chain, the Member needs a method to assess or differentiate between levels of risk. A simple method is assigning the level of risk between low, medium, and high. CTPAT developed the Five Step Risk Assessment guide as an aid to conducting the international risk assessment portion of a Member's overall risk assessment, and it can be found on U.S. Customs and Border Protection's website at https://www.cbp.gov/sites/default/files/documents/C-TPAT%27s%20Five%20Step%20Risk%20Assessment%20Process.pdf. For Members with extensive supply chains, the primary focus is expected to be on areas of higher risk.	Must

ID	Criteria	Implementation Guidance	Must / Should
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
2.3	Risk assessments must be reviewed annually, or more frequently as risk factors dictate.	Circumstances that may require a risk assessment to be reviewed more frequently than once a year include an increased threat level from a specific country, periods of heightened alert, following a security breach or incident, changes in business partners, and/or changes in corporate structure/ownership such as mergers and acquisitions etc.	Must
2.4	CTPAT Members should have written procedures in place that address crisis management, business continuity, security recovery plans, and business resumption.	A crisis may include the disruption of the movement of trade data due to a cyberattack, a fire, or a carrier driver being hijacked by armed individuals. Based on risk and where the Member operates or sources from, contingency plans may include additional security notifications or support; and how to recover what was destroyed or stolen to return to normal operating conditions.	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 fulfill 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.	Must

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 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.	Must

ID	Criteria	Implementation Guidance	Must / Should
		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. *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).	

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 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

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

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, 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.	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, 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.

ID	Criteria	Implementation Guidance	Must / Should
4.1	CTPAT Members must have comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems. The written IT policy, at a minimum, must cover all of the individual cybersecurity criteria.	Members are encouraged to follow cybersecurity protocols that are based on recognized industry frameworks/standards. The *National Institute of Standards and Technology (NIST) is one such organization that provides a Cybersecurity Framework (https://www.nist.gov/cyberframework) that offers voluntary guidance based upon existing standards, guidelines, and practices to help manage and reduce cybersecurity risks both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. The Framework complements an organization's risk management process and cybersecurity program. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one. *NIST is a non-regulatory federal agency under the Department of Commerce that promotes and maintains measurement standards, and it is the technology standards developer for the federal government.	Must

ID	Criteria	Implementation Guidance	Must / Should
4.2	To defend Information Technology (IT) systems against common cybersecurity threats, a company must install sufficient software/hardware protection from malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewalls) in Members' computer systems. Members must ensure that their security software is current and receives regular security updates. Members must have policies and procedures to prevent attacks via social engineering. If a data breach occurs or another unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and/or data.		Must
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

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

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 passwords or stolen credentials. MFAs can assist in closing these attack vectors by requiring individuals to augment passwords or passphrases (something you know) with something you have, like a token, or one of your physical features - a biometric. If using passwords, they need to be complex. The National Institute of Standards and Technology's (NIST) NIST Special Publication 800-63B: Digital Identity Guidelines, includes password guidelines (https://pages.nist.gov/800-63-3/sp800-63b.html). It recommends the use of long, easy to remember passphrases instead of words with special characters. These longer passphrases (NIST recommends allowing up to 64 characters in length) are considered much harder to crack because they are made up of an easily memorized sentence or phrase.	Must
4.9	Members that allow their users to remotely connect to a network must employ secure technologies, such as virtual private networks (VPNs), to allow employees to access the company's intranet securely when located outside of the office. Members must also have procedures designed to prevent remote access from unauthorized users.	VPNs are not the only choice to protect remote access to a network. Multi-factor authentication (MFA) is another method. An example of a multi-factor authentication would be a token with a dynamic security code that the employee must type in to access the network.	Must

ID	Criteria	Implementation Guidance	Must / Should
4.10	If Members allow employees to use personal devices to conduct company work, all such devices must adhere to the company's cybersecurity policies and procedures to include regular security updates and a method to securely access the company's network.	Personal devices include storage media like CDs, DVDs, and USB flash drives. Care must be taken if employees are allowed to connect their personal media to individual systems since these data storage devices may be infected with malware that could propagate using the company's network.	Must
4.11	Cybersecurity policies and procedures should include measures to prevent the use of counterfeit or improperly licensed technological products.	Computer software is intellectual property (IP) owned by the entity that created it. Without the express permission of the manufacturer or publisher, it is illegal to install software, no matter how it is acquired. That permission almost always takes the form of a license from the publisher, which accompanies authorized copies of software. Unlicensed software is more likely to fail as a result of an inability to update. It is more prone to contain malware, rendering computers and their information useless. Expect no warranties or support for unlicensed software, leaving your company on its own to deal with failures. There are legal consequences for unlicensed software as well, including stiff civil penalties and criminal prosecution. Software pirates increase costs to users of legitimate, authorized software and decrease the capital available to invest in research and development of new software. Members may want to have a policy that requires product key labels and certificates of authenticity to be kept when new media is purchased. CDs, DVDs, and USB media include holographic security features to help ensure you receive authentic products and to protect against counterfeiting.	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 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
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 of Standards 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