# Minimum Security Criteria – Highway Carriers

**March 2020**

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

## 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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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 |
|---|---|---|---|
| 2.3 | 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:<br>• Verifying the company's business address and how long they have been at that address;<br>• Conducting research on the internet on both the company and its principals;<br>• Checking business references; and<br>• Requesting a credit report.<br><br>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 |
| 3.3 | Written screening processes must include indicators to identify shipments or customers that might not be legitimate. If a higher risk factor is flagged when screening a shipment/customer, the carrier must complete a more in depth review. If the vetting leads to substantial doubt to the veracity of the shipment/customer, the carrier must notify U.S. Customs and Border Protection of its suspicions. | Some of the warning signs could be willing to pay above the standard rate, in cash; having little knowledge of the commodity to be shipped; being evasive; minimal contact information (cell phone, P.O. box); new business/no business history, etc. | 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.<br><br>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.<br><br>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.<br><br>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.<br><br>Determining if a business partner is compliant with the MSC can be accomplished in several ways. Based on risk, the company | Must |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| | | 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:<br><br>•Name and title of the person(s) completing it;<br>•Date completed;<br>•Signature of the individual(s) who completed the document;<br>•*Signature of a senior company official, security supervisor, or authorized company representative to attest to the accuracy of the questionnaire;<br>•Provide enough detail in responses to determine compliance; and<br>•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.<br><br>*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 |
|---|---|---|---|
| 3.7 | 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.<br><br>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.<br><br>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 |
|---|---|---|---|
| 3.8 | For inbound shipments to the United States, if a Member subcontracts transportation services to another highway carrier, the Member must use a CTPAT certified highway carrier or a highway carrier that works directly for the Member as delineated through a written contract. The contract must stipulate adherence to all minimum security criteria (MSC) requirements. | The carrier should provide a list of subcontracted carriers and drivers to the facilities where it picks up and delivers cargo. Any changes to the subcontractor list should be immediately conveyed to relevant partners.<br><br>When reviewing service providers for compliance, the Member should verify that the company subcontracted is actually the company transporting the loads—and has not further subcontracted loads without approval.<br><br>Members should limit subcontracting transportation services to one level only. If exceptions are allowed for further subcontracting, the CTPAT Member and the shipper should be notified that the load was further subcontracted. | 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 | 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.<br><br>*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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>Media Sanitization:<br>https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization | 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 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.

   At the point of stuffing/loading, procedures need to be in place to inspect IIT and properly seal them. Cargo in transit or "at rest" is under less control, and is therefore more vulnerable to infiltration, which is why seal controls and methods to track cargo/conveyances in transit are key security criteria.

   Breaches in supply chains occur most often during the transportation process; therefore, Members must be vigilant that these key cargo criteria be upheld throughout their supply chains.

   **Key Definition: Instruments of International Traffic (IIT) –** IIT include containers, flatbeds, unit load devices (ULDs), lift vans, cargo vans, shipping tanks, bins, skids, pallets, caul boards, cores for textile fabrics, or other specialized containers arriving (loaded or empty), in use or to be used in the shipment of merchandise in international trade.

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| 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 |
| 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, 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. | Must |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| | | 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.). | |
| 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.<br><br><u>Inspection requirements for CTPAT shipments via ocean, air, and land borders (as applicable) by rail or intermodal freight:</u><br><br>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 refrigerated containers and ULDs:<br><br>1. Front wall;<br>2. Left side;<br>3. Right side;<br>4. Floor;<br>5. Ceiling/Roof;<br>6. Inside/outside doors, including the reliability of the locking mechanisms of the doors;<br>7. Outside/Undercarriage; and<br>8. Fan housing on refrigerated containers. | 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.<br><br>Expectations for overseas supply chains are to inspect all 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.<br><br>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).<br><br>The Public Library Section of the CTPAT Portal contains training material on security and agricultural conveyance/Instruments of International Traffic inspections. | Must |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| | <u>Additional inspection requirements for land border crossings via highway carriers:</u><br><br>Inspections of conveyances and IIT must be conducted at conveyance/IIT storage yards.<br><br>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:<br><br>**<u>Tractors:</u>**<br><br>1. Bumper/tires/rims;<br>2. Doors, tool compartments and locking mechanisms;<br>3. Battery box;<br>4. Air breather;<br>5. Fuel tanks;<br>6. Interior cab compartments/sleeper; and<br>7. Faring/roof.<br><br>**<u>Trailers</u>**:<br><br>1. Fifth wheel area - check natural compartment/skid plate;<br>2. Exterior - front/sides;<br>3. Rear - bumper/doors;<br>4. Front wall;<br>5. Left side;<br>6. Right side;<br>7. Floor;<br>8. Ceiling/roof;<br>9. Inside/outside doors and locking mechanisms; and<br>10.Outside/Undercarriage. | | |

| 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 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 |
| 5.5 | The inspection of all conveyances and empty Instruments of International Traffic should be recorded on a checklist. The following elements should be documented on the checklist:<br><br>• Container/Trailer/Instruments of International Traffic number;<br>• Date of inspection;<br>• Time of inspection;<br>• Name of employee conducting the inspection; and<br>• Specific areas of the Instruments of International Traffic that were inspected.<br><br>If the inspections are supervised, the supervisor should also sign the checklist.<br><br>The completed container/Instruments of International Traffic inspection sheet should be part of the shipping documentation packet. The consignee should receive the complete shipping documentation packet prior to receiving the merchandise. | | Should |
| 5.6 | All security inspections should be performed in an area of controlled access and, if available, monitored via a CCTV system. | | Should |
| 5.7 | If visible pest contamination is found during the conveyance/Instruments of International Traffic inspection, washing/vacuuming must be carried out to remove such contamination. Documentation must be retained for one year to demonstrate compliance with these inspection requirements. | Keeping records on the types of contaminants found, where they were found (conveyance location), and how the pest contamination was eliminated, are helpful actions that may assist Members in preventing future pest contamination. | Must |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| 5.8 | Based on risk, management personnel should conduct random searches of conveyances after the transportation staff have conducted conveyance/Instruments of International Traffic inspections.<br><br>The searches of the conveyance should be done periodically, with a higher frequency based on risk. The searches should be conducted at random without warning, so they will not become predictable. The inspections should be conducted at various locations where the conveyance is susceptible: the carrier yard, after the truck has been loaded, and en route to the United States border. | Supervisory searches of conveyances are conducted to counter internal conspiracies.<br><br>As a best practice, supervisors can hide an item (like a toy or colored box) in the conveyance to determine if the field test screener/conveyance operator finds it.<br><br>Supervisory personnel could be a security manager, held accountable to senior management for security, or other designated management personnel. | Should |
| 5.11 | A tracking and monitoring activity log or equivalent technology (such as GPS) must be used to track the conveyance while it is en route to the United States. If driver logs are used, the driver must record any stops and note that inspections of the conveyance, Instruments of International Traffic (IIT), and the seal were conducted. | Conveyances are tracked to prevent them from being diverted to tamper with the load or structure of the conveyance/Instruments of International Traffic to allow contraband to be introduced in the shipment. Based on risk, transportation providers may want to track and monitor their conveyances/Instruments of International Traffic in real time. There are many tracking tools available to users free of charge via their smart cell phones. For small carriers, applications such as Life 360, Find Friends from Google, and WhatsApp allow users to track people and conveyances. | Must |
| 5.14 | CTPAT Members should work with their transportation providers to track conveyances from origin to final destination point. Specific requirements for tracking, reporting, and sharing of data should be incorporated within terms of service agreements with service providers. | | Should |
| 5.16 | For land border shipments that are in proximity to the United States border, a “no-stop” policy should be implemented with regard to unscheduled stops. | Cargo at rest is cargo at risk. Scheduled stops would not be covered by this policy, but would have to be considered in an overall tracking and monitoring procedure. | Should |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| 5.19 | If a GPS tracking system is used, carriers should use a sensor coupling/connector or equivalent technology from the tractor to the trailer to ensure the trailer is also monitored and tracked. | | Should |
| 5.20 | Carriers should use electronic dispatch logs; the logs should be recorded and kept for audit purposes. | Electronic dispatch logs provide a more accessible means of conducting management oversight and enabling information to be shared and/or compared with additional assessment data. It is recommended that records of the logs be maintained for a sufficient amount of time to allow for audits to be conducted and for investigative purposes, if a breach were to occur in a supply chain. | Should |
| 5.21 | For cross-border shipments, pre-designated transit routes must be established, which include anticipated transit times between waypoints. Once the time between the assigned points has been determined, for both peak and non-peak times, these times must be recorded and incorporated into the tracking process.<br><br>If GPS technology is employed, geo-fencing must be implemented to include alarm notification when a carrier deviates from the assigned route. The parameters for geo-fencing must be set at minimal allowable tolerances for the pre-established transit route. | Waypoints are specific geographical locations defined by sets of coordinates -longitude and latitude- used for navigational purposes, including driving or transit routes.<br><br>It is recommended waypoints include the length of time between the yard to the loading point/trailer pickup, the U.S. border, and the delivery destinations. If a stop is made to collect export documents or to verify seals, these can also be included as waypoints. | Must |
| 5.22 | Carriers must have systems or written procedures in place to respond to significant route deviations and late arrivals to the loading dock/area, transfer points, or the final destination. Drivers must notify the dispatcher of any significant route delays due to weather, traffic, and/or rerouting. Dispatch must independently verify the cause of the delay. | | Must |
| 5.23 | After a stop, drivers must inspect the conveyance's sealing or locking devices for any signs of tampering prior to resuming the trip. These inspections must be documented. | | Must |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| 5.24 | In areas of high risk, and immediately prior to arrival at the border crossing, CTPAT Members should incorporate a "last chance" verification process for U.S. bound shipments for checking conveyances/Instruments of International Traffic for signs of tampering to include visual inspections of conveyances and the VVTT seal verification process. Properly trained individuals should conduct the inspections.<br><br>V – View seal and container locking mechanisms; ensure they are OK;<br>V – Verify seal number against shipment documents for accuracy;<br>T – Tug on seal to make sure it is affixed properly;<br>T – Twist and turn the bolt seal to make sure its components do not unscrew, separate from one another, or any part of the seal becomes loose. | | Should |
| 5.26 | Drivers must report and record any anomalies or unusual structural modifications found on the conveyance following a Government inspection. | These include U.S. Department of Transportation (DOT) inspections or other regulatory agency inspections. It also includes inspections taking place in Mexico and Canada. | Must |
| 5.27 | Management must regularly conduct random reviews of the tracking and monitoring procedures. The review findings must be recorded. The review must cover verification of the tracking log against time-indicative documents and internal systems; unaccounted transit time lapses must also be included. Management should conduct periodic random verifications en route. | Random reviews are required to ensure tracking logs are properly maintained and conveyance tracking and monitoring procedures are being followed. Time-indicative documents include fuel receipts, scale logs, toll receipts, ACE, Mexico SAT, broker status information, etc. Conducting en route verifications is a measure used in high risk areas to verify procedures are being followed in "real time." | Must |
| 5.28 | CTPAT highway carriers should notify appropriate parties (e.g., shipper, consignee, and importer) of any significant delays including mechanical failures during transit. | | 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 |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| 5.30 | Any technology, to include transponders, provided by CBP to the highway carrier, must be protected against misuse, compromise, theft, tampering, altering or duplication. Any misuse of transponders, to include procuring them for external carriers, will result in suspension or removal from the program. Moreover, in order to decrease wait times, CTPAT carriers must either pay the annual user fee or the single-crossing user fee online prior to arrival at a port of entry. | The transponder, also known as a User Fee, is a sticker that contains a radio-frequency identification chip (RFID technology) that transmits information about a vehicle and border crossing User Fee payment status. The transponder is attached to the windshield of a commercial vehicle and should remain on the vehicle for the life of the transponder (up to 10 years), even if the vehicle is sold. For more on transponders, consult the Decal and Transportation Online Procurement System (DTOPS): https://dtops.cbp.dhs.gov<br><br>Paying the annual user fee or the single-crossing user fee online prior to arriving at the border reduces fuel consumption and wait times. Removing the cash/credit card payment process from primary inspection enables CBP officers to process vehicles faster and decreases carbon emissions associated with heavy traffic. | 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.<br><br>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.<br><br>Written seal controls must include the following elements:<br><br>**Controlling Access to Seals**:<br>• Management of seals is restricted to authorized personnel.<br>• Secure storage.<br><br>**Inventory, Distribution, & Tracking (Seal Log):**<br>• Recording the receipt of new seals.<br>• Issuance of seals recorded in log.<br>• Track seals via the log.<br>• Only trained, authorized personnel may affix seals to Instruments of International Traffic (IIT).<br><br>**Controlling Seals in Transit**:<br>• When picking up sealed IIT (or after stopping) verify the seal is intact with no signs of tampering.<br>• Confirm the seal number matches what is noted on the shipping documents.<br>Seals Broken in Transit: | | Must |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| | • If a load is examined, record the replacement seal number.<br>• The driver must immediately notify dispatch when a seal is broken, indicate who broke the seal, and provide the new seal number.<br>• The carrier must immediately notify the shipper, broker, and importer of the seal change and the replacement seal number.<br>• The shipper must note the replacement seal number in the seal log.<br><br>**Seal Discrepancies:**<br>• Retain altered or tampered seals to aid in investigations.<br>• Investigate the discrepancy; follow-up with corrective measures (if warranted).<br>• 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 |
| 6.3 | Less Than Truck Load (LTL) carriers must (at the very least) use a high-security padlock when picking up local freight in an international LTL environment where consolidation hubs are not used. At the last pickup site prior to crossing the border, the carrier must seal the load with an ISO 17712 compliant high-security seal.<br><br>LTL carriers must have strict controls limiting access to padlocks, keys, or combinations that can open the padlocks. | | Must |

| 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.<br><br>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:<br><br>V – View seal and container locking mechanisms; ensure they are OK;<br>V – Verify seal number against shipment documents for accuracy;<br>T – Tug on seal to make sure it is affixed properly;<br>T – Twist and turn the bolt seal to make sure its components do not unscrew, separate from one another, or any part of the seal becomes loose. | 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 |

7. **Procedural Security** – Procedural Security encompasses many aspects of the import-export process, documentation, and cargo storage and handling requirements. Other vital procedural criteria pertain to reporting incidents and notification to pertinent law enforcement. Additionally, CTPAT often requires that procedures be written because it helps maintain a uniform process over time. Nevertheless, the amount of detail needed for these written procedures will depend upon various elements such as a company's business model or what is covered by the procedure.

   CTPAT recognizes that the technology used in supply chains continues to evolve. The terminology used throughout the criteria references written, paper-based procedures, documents, and forms. Electronic documents and signatures, and other digital technologies, however, are also acceptable ways to document required procedures.
   The CTPAT program is not designed to be a "one size fits all" model. Each company must decide (based on its risk assessment) how to implement and maintain procedures. However, it is more effective to incorporate security processes within existing procedures rather than create a separate manual for security protocols. This creates a more sustainable structure and helps emphasize that supply chain security is everyone's responsibility.

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| 7.2 | Cargo staging areas, and the immediate surrounding areas, must be inspected on a regular basis to ensure these areas remain free of visible pest contamination. | Preventative measures such as the use of baits, traps, or other barriers can be used as necessary. Removal of weeds or reduction of overgrown vegetation may help in the elimination of pest habitat within staging areas. | Must |
| 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 |

| ID | Criteria | Implementation Guidance | Must / 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 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.<br><br>Requiring the seal number to be electronically printed on the bill of lading (BOL) or other export documents helps guard against changing the seal and altering the pertinent document(s) to match the new seal number.<br><br>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 |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| 7.10 | Personnel must review the information included in import/export documents to identify or recognize suspicious cargo shipments.<br><br>Relevant personnel must be trained on how to identify information in shipping documents, such as manifests, that might indicate a suspicious shipment.<br><br>Based on risk, CTPAT Members should take into account those CTPAT key warning indicators for money laundering and terrorism financing activities most applicable to the functions that they and/or their business entities perform in the supply chain. A document on key warning indicators is available in the CTPAT Portal (Public Library section).<br><br>Highway carrier personnel must be trained to review manifests and other documents in order to identify or recognize suspicious cargo shipments such as those that:<br><br>• Originate from or have unusual destination locations;<br>• Are paid by cash or a certified check;<br>• Use unusual routing methods;<br>• Exhibit unusual shipping/receiving practices;<br>• Provide vague, generalized, or a lack of information. | | Must |
| 7.12 | Drivers must collect personal garbage and dispose of it before entering the United States. Otherwise, the driver must declare it to U.S. Customs and Border Protection, so it may be properly disposed. | | Must |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| 7.13 | Based on risk, highway carriers must have specific procedures in place to mitigate the risk of collusion between employees, such as between driver and dispatch personnel, which might allow a security measure to be overcome. | An example of an internal conspiracy would be a driver and dispatch staff colluding to falsify travel times to undermine tracking and monitoring procedures. Procedures to prevent collusion may include assignment rotation, restricted driver access to physical location of dispatcher operations, separate break rooms for dispatch staff and drivers, placement of GPS monitors out of the drivers' view, frequent documented audits of dispatcher logs, and trend analysis using GPS data to compare drivers' average time against which dispatch staff members are on duty. | Must |
| 7.14 | If legally allowed, and permissible under union rules, carriers should conduct random screening of truck drivers' luggage and personal belongings. If any suspicious anomalies are found during the screening, the carrier should document and report its findings to U.S. Customs and Border Protection. | | Should |
| 7.15 | CTPAT highway carriers must ensure their FAST certified drivers follow all FAST requirements when using the FAST lane, to include only having passengers in the cabin of the truck that are FAST certified. | | Must |
| 7.16 | For U.S. bound shipments, the highway carrier transporting the cargo (including subcontracted carriers) must use its own SCAC code regardless of whether the carrier is using a FAST or regular lane. | | Must |
| 7.17 | In accordance with U.S. Department of Transportation standards, CTPAT highway carriers should have a comprehensive vehicle preventive maintenance program in place and ensure the drivers are performing adequate checks of their vehicles. Maintenance records should be kept for a minimum of one year. | Cargo at rest is cargo at risk. A comprehensive maintenance program may help avoid unforeseen stops due to mechanical issues. | Should |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| 7.18 | In areas of high risk, where operationally feasible, the highway carrier should use a convoy method (e.g., a minimum of two trucks traveling together) to transport cargo. Each truck in the convoy should have the means to communicate with the other trucks in the convoy and with the dispatch staff. | | Should |
| 7.23 | CTPAT Members must have written procedures for reporting an incident, which includes a description of the facility's internal escalation process.<br><br>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 chain. Notifications to CBP must be made as soon as feasibly possible and in advance of any conveyance or IIT crossing the border.<br><br>Notification procedures must include the accurate contact information that lists the name(s) and phone number(s) of personnel requiring notification, as well as for law enforcement agencies. Procedures must be periodically reviewed to ensure contact information is accurate. | Examples of incidents warranting notification to U.S. Customs and Border Protection include (but are not limited to) the following:<br><br>• Discovery of tampering with a container/IIT or high-security seal;<br>• Discovery of a hidden compartment in a conveyance or IIT;<br>• An unaccounted new seal has been applied to an IIT;<br>• Smuggling of contraband, including people; stowaways;<br>• Unauthorized entry into conveyances, locomotives, vessels, or aircraft carriers;<br>• Extortion, payments for protection, threats, and/or intimidation;<br>• Unauthorized use of a business entity identifier (i.e., Importer of Record (IOR) number, Standard Carrier Alpha (SCAC) code, etc.). | Must |
| 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 |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| 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 conspiracies may be reported more readily if the reporting party knows the concern may be reported anonymously.<br><br>Members can set up a hotline program or similar mechanism that allows people to remain anonymous if they fear reprisal for their actions. It is recommended that any report be kept as evidence to document that each reported item was investigated and that corrective actions were taken. | Should |
| 7.30 | Seal numbers should be electronically printed on the bill of lading or other shipping documents. | | Should |
| 7.31 | CTPAT highway carriers (or an authorized party transmitting on behalf of the carrier) must transmit an electronic manifest for bobtails and for empty containers/trailers prior to the arrival of the conveyance at the U.S. Customs and Border Protection primary booth using the Automated Commercial Environment (ACE) Electronic Truck Manifest (e-Manifest) system. | The Trade Act of 2002 does not require highway carriers to transmit electronic information in advance to U.S. Customs and Border Protection on empty containers – only for loaded ones. CTPAT is requiring that the carrier submit the conveyance and driver information before the truck arrives at a U.S. Customs and Border Protection booth. | Must |
| 7.33 | If transponders are used, highway carriers must have a written procedure in place to manage the ordering, issuance, activation, and deactivation of transponders. CTPAT highway carriers are prohibited from requesting transponders for any highway carrier that is not owned and controlled by the member highway carrier. | | Must |
| 7.37 | Following a significant security incident, Members must initiate a post-incident analysis immediately after becoming aware of the incident and in order to determine where the supply chain may have been compromised. This analysis must not impede/interfere with any known investigations conducted by a government law enforcement agency. The company's post-incident analysis findings must be documented, completed as soon as feasibly possible, and, if allowed by law enforcement authorities, made available to the SCSS upon request. | A security incident is a breach in which security measures have been circumvented, eluded, or violated, and have resulted or will result in a criminal act. Security incidents include acts of terrorism, smuggling (narcotics, human, etc.), and the presence of stowaways. | Must |

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 or treatments. Ensuring compliance with CTPAT's agricultural requirements will also help protect a key industry in the U.S. and the overall global food supply.

**Key Definition: Pest contamination** – The International Maritime Organization defines pest contamination 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.).

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| 8.1 | CTPAT Members must, in accordance with their business model, have written procedures designed to prevent visible pest contamination to include compliance with Wood Packaging Materials (WPM) regulations. Visible pest prevention measures must be adhered to throughout the supply chain. Measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15). | WPM is defined as wood or wood products (excluding paper products) used in supporting, protecting, or carrying a commodity. WPM includes items such as pallets, crates, boxes, reels, and dunnage. Frequently, these items are made of raw wood that may not have undergone sufficient processing or treatment to remove or kill pests, and therefore remain a pathway for the introduction and spread of pests. Dunnage in particular has been shown to present a high risk of introduction and spread of pests.<br><br>The IPPC is a multilateral treaty overseen by the United Nation's Food and Agriculture Organization that aims to secure coordinated, effective action to prevent and to control the introduction and spread of pests and contaminants.<br><br>ISPM 15 includes internationally accepted measures that may be applied to WPM to reduce significantly the risk of introduction and spread of most pests that may be associated with WPM. ISPM 15 affects all wood packaging material requiring that they be debarked and then heat treated or fumigated with methyl bromide and stamped or branded with the IPPC mark of compliance. This mark of compliance is colloquially known as the "wheat stamp". Products exempt from the ISPM 15 are made from alternative materials, like paper, metal, plastic or wood panel products (i.e. oriented strand board, hardboard, and plywood). | Must |

## 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 enter or exit (as well as other points of egress) must be manned or monitored. Individuals and vehicles may be subject to search in accordance with local and labor laws. | It is recommended that the number of gates be kept to the minimum necessary for proper access and safety. Other points of egress would be entrances to facilities that are not gated. | Must |
| 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 |

| ID | Criteria | Implementation Guidance | Must / 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.<br><br>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 |
| 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.<br><br>At a minimum, these policies and procedures must stipulate:<br><br>• That access to the locations where the technology is controlled or managed is limited to authorized personnel;<br><br>• The procedures that have been implemented to test/inspect the technology on a regular basis; | Security technology needs to be tested on a regular basis to ensure it is working properly. There are general guidelines to follow:<br><br>• 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.<br><br>• 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 | Must |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| | • That the inspections include verifications that all of the equipment is working properly, and if applicable, that the equipment is positioned correctly;<br><br>• That the results of the inspections and performance testing is documented;<br><br>• That if corrective actions are necessary, they are to be implemented as soon as possible and the corrective actions are documented;<br><br>• That the documented results of these inspections be maintained for a sufficient time for audit purposes.<br><br>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.<br><br>Security technology policies and procedures must be reviewed and updated annually, or more frequently, as risk or circumstances dictate. | center should be double-checked.<br><br>• Make sure video settings such as motion activated recording; motion detection alerts; images per second (IPS), and quality level, have been set up properly.<br><br>• 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.<br><br>• Test to make sure security cameras are positioned correctly and remain in the proper position (cameras may have been deliberately or accidentally moved). | |
| 9.9 | CTPAT Members should use licensed/certified resources when considering the design and installation of security technology. | Today's security technology is complex and evolves rapidly. Oftentimes companies purchase the wrong security technology that proves to be ineffective when needed and/or pay more than was necessary. Seeking qualified guidance will help a buyer select the right technology options for their needs and budget.<br><br>According to the National Electrical Contractors Association (NECA), in the U.S. 33 states currently have licensing requirements for professionals engaged in the installation of security and alarm systems. | Should |

| 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 alternative power source that will allow the systems to continue to operate in the event of an unexpected loss of direct power. | A criminal trying to breach your security may attempt to disable the power to your security technology in order to circumnavigate it. Thus, it is important to have an alternative source of power for your security technology. An alternative power source may be an auxiliary power generation source or backup batteries. Backup power generators may also be used for other critical systems such as lighting. | Should |
| 9.12 | If camera systems are deployed, cameras should monitor a facility's premises and sensitive areas to deter unauthorized access. Alarms should be used to alert a company to unauthorized access into sensitive areas. | Sensitive areas, as appropriate, may include cargo handling and storage areas, shipping/receiving areas where import documents are kept, IT servers, yards and storage areas for Instruments of International Traffic (IIT), areas where IIT are inspected, and seal storage areas. | Should |
| 9.13 | If camera systems are deployed, cameras must be positioned to cover key areas of facilities that pertain to the import/export process.<br><br>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.<br><br>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 |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| 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 |
|---|---|---|---|
| 9.15 | 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 include any corrective actions taken. The results must be maintained for a sufficient time for audit purposes. | If camera footage is only reviewed for cause (as part of an investigation following a security breach etc.), the full benefit of having cameras is not being realized. Cameras are not only investigative tools. If used proactively, they may help prevent a security breach from occurring in the first place.<br><br>Focus the random review of the footage on the physical chain of custody to ensure the shipment remained secure and all security protocols were followed. Some examples of processes that may be reviewed are the following:<br><br>• Cargo handling activities;<br>• Container inspections;<br>• The loading process;<br>• Sealing process;<br>• Conveyance arrival/exit; and<br>• Cargo departure, etc.<br><br>**Purpose of the review:** The review is intended to evaluate overall adherence and effectiveness of established security processes, identify gaps or perceived weaknesses, and prescribe corrective actions in support of improvement to security processes. Based on risk (previous incidents or an anonymous report on an employee failing to follow security protocols at the loading dock, etc.), the Member may target a review periodically.<br><br>**Items to include in the written summary**:<br>• The date of the review;<br>• Date of the footage that was reviewed;<br>• Which camera/area was the recording from;<br>• Brief description of any findings; and<br>• If warranted, corrective actions. | Must |

| 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.<br><br>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.** **Physical Access Controls** – 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.<br><br>Where applicable, a personnel identification system must be in place for positive identification and access control purposes. Access to sensitive areas must be restricted based on job description or assigned duties. Removal of access devices must take place when the employees separate from 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 system is required. | Must |

| 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.<br><br>The registration log must include the following:<br><br>• Date of the visit;<br>• Visitor's name;<br>• 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;<br>• Time of arrival;<br>• Company point of contact; and<br>• Time of departure. | | Must |
| 10.3 | Drivers delivering or receiving cargo must be positively identified before cargo is received or released. Drivers must present government-issued photo identification to the facility employee granting access to verify their identity. If presenting a government-issued photo identification is not feasible, the facility employee may accept a recognizable form of photo identification issued by the highway carrier company that employs the driver picking up the load. | | Must |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| 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.<br><br>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 |
| 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 |
| 10.10 | 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 |

**11. <u>Personnel Security</u> –** A company's human resource force is one of its most critical assets, but it may also be one of its weakest security links. The criteria in this category focus on issues such as employee screening and pre-employment verifications. Many security breaches are caused by internal conspiracies, which is where one or more employees collude to circumvent security procedures aimed at allowing an infiltration of the supply chain. Therefore, Members must exercise due diligence to verify that employees filling sensitive positions are reliable and trustworthy. Sensitive positions include staff working directly with cargo or its documentation, as well as personnel involved in controlling access to sensitive areas or equipment. Such positions include, but are not limited to, shipping, receiving, mailroom personnel, drivers, dispatch, security guards, any individuals involved in load assignments, tracking of conveyances, and/or seal controls.

| 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 countries may not allow all of the application information to be verified. However, due diligence is expected to verify application information when permitted. | Must |

| 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.<br><br>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. 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 training program must be comprehensive and cover all of CTPAT's security requirements. Personnel in sensitive positions must receive additional specialized training geared toward the responsibilities that the position holds.<br><br>One of the key aspects of a security program is training. Employees who understand why security measures are in place are more likely to adhere to them. Security training must be provided to employees, as required, based on their functions and position on a regular basis, and newly hired employees must receive this training as part of their orientation/job skills training.<br><br>Members must retain evidence of training such as training logs, sign in sheets (roster), or electronic training records. Training records should include the date of the training, names of attendees, and the topics of the training. | Training topics may include protecting access controls, recognizing internal conspiracies, and reporting procedures for suspicious activities and security incidents. When possible, specialized training should include a hands-on demonstration. If a hands-on demonstration is conducted, the instructor should allow time for the students to demonstrate the process.<br><br>For CTPAT purposes, sensitive positions include staff working directly with import/export cargo or its documentation, as well as personnel involved in controlling access to sensitive areas or equipment. Such positions include, but are not limited to, shipping, receiving, mailroom personnel, drivers, dispatch, security guards, any individuals involved in load assignments, tracking of conveyances, and/or seal controls. | Must |

| ID | Criteria | Implementation Guidance | Must / Should |
|---|---|---|---|
| 12.2 | Drivers and other personnel that conduct security and agricultural inspections of empty conveyances and Instruments of International Traffic (IIT) must be trained to inspect their conveyances/IIT for both security and agricultural purposes.<br><br>Refresher training must be conducted periodically, as needed after an incident or security breach, or when there are changes to company procedures.<br><br>Inspection training must include the following topics:<br>• Signs of hidden compartments;<br>• Concealed contraband in naturally occurring compartments; and<br>• Signs of pest contamination. | | Must |
| 12.3 | Personnel must receive training on situational reporting – the procedures to follow if something is found during a conveyance inspection or if a security incident takes place while in transit. In addition, personnel must be instructed in controlling/using seals during transit, and to look for signs of someone observing the movement of the conveyance and/or the goods.<br><br>Drivers, for instance, must be trained on how to conduct the seal verification process (VVTT process).<br><br>The CTPAT seal verification process is the following:<br><br>V – View seal and container locking mechanisms; ensure they are OK;<br>V – Verify seal number against shipment documents for accuracy;<br>T – Tug on seal to make sure it is affixed properly; and<br>T – Twist and turn the bolt seal to make sure its components do not unscrew or separate from one another. | | Must |

| 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 one's position (for sensitive employees) is of paramount importance. Exams or quizzes, a simulation exercise/drill, or regular audits of procedures etc. are some of the measures that the Member may implement to determine the effectiveness of the training. | Should |
| 12.7 | Training must, in accordance with the Member's business model, be provided to applicable personnel on preventing visible pest contamination. Training must encompass pest prevention measures, regulatory requirements applicable to wood packaging materials (WPM), and identification of infested wood. | U.S. Customs and Border Protection has collaborated with the U.S. Department of Agriculture to develop training on visible pest contamination. Different training modules have been developed for the different trade environments: air, sea, and land border (rail and highway carrier). These training modules will be made available to all Members via the CTPAT Portal. | Must |
| 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-training via operational manuals and other methods is acceptable. | | Must |
| 12.10 | Personnel must be trained on how to report security incidents and suspicious activities. | Procedures to report security incidents or suspicious activity are extremely important aspects of a security program. Training on how to report an incident can be included in the overall security training. Specialized training modules (based on job duties) may have more detailed training on reporting procedures, including specifics on the process, such as, what to report, to whom, how to report the incident, and what to do after the report is completed. | Must |