A Message Regarding Security Procedures Guidelines for

Consolidators, Carrier-Forwarders and Highway Carriers

(Additional Industrial sectors included: Highway / Sea / Air / Rail Carriers / NVOCCs)

Tricar Sales Inc. is a participant in the Customs-Trade Partnership Against Terrorism (CTPAT) program of the United States Customs & Border Patrol agency (CBP).

CTPAT is a voluntary joint government-business initiative to build cooperative relationships that strengthen the overall supply chain and border security. Everyone involved in logistics, distribution, or supply chain management will be impacted by ongoing efforts to create a more secure global trading system. **The CTPAT program is similar to Authorized Economic Operator (AEO) security programs in many other countries around the world.**

Importers such as our company are expected to complete a security assessment of our entire supply chain. The assessment must include the security-related subjects of:

Access Control
Agricultural Procedures
Business Partners
Conveyance Security
Information Technology
Personnel Security
Physical Security
Procedural Security
Security Awareness Training
Trade-Based Money Laundering
Upper Management Responsibility

As our business partner, it is necessary for your company to have and continuously seek to improve upon security processes and procedures consistent with CTPAT security criteria. Hence, we request that you provide one (only) of the following documents to verify compliance with CTPAT security-procedures guidelines.

- Copy of CTPAT Certification (only for CTPAT certified companies).
- Certification of participation in a foreign Customs security program.
- Documentation from a corporate officer attesting to compliance.
- Completion of a security questionnaire for your industrial sector.

Please provide this information to us as soon as you receive this letter. If you should have any questions, please contact us by replying to the email by which you received this message, or at telephone number: (520)-987-2981.

Regarding the CTPAT program and security concerns, for your convenience we also included the below CTPAT security-procedures guidelines for Highway, Sea, Air and Rail Carriers and NVOCCs, so that you may forward them to your business partners.

Thank you for your assistance with this very important matter.

Best regards,
Tricar Sales Inc.

Instructions: Please find and refer to your Industrial sector.

Consolidators & Carrier-Forwarders

CTPAT Security Procedures Guidelines

Consolidators must conduct a comprehensive assessment of their international supply chains based upon the following CTPAT security procedures guidelines. Where a consolidator outsources or contracts elements of their supply chain, such as a foreign facility, conveyance, domestic warehouse, or other elements, the consolidator must work with these business partners to ensure that pertinent security measures are in place and adhered to throughout their supply chain. The supply chain for CTPAT purposes is defined from point of origin (manufacturer/supplier/vendor) through to point of distribution and recognizes the diverse business models CTPAT members employ.

CTPAT recognizes the complexity of international supply chains and endorses the application and implementation of security measures based upon risk analysis. Therefore, the program allows for flexibility and the customization of security plans based on the member's business model. Appropriate security measures, as listed throughout this document, must be implemented, and maintained throughout the consolidator's supply chains.

Business Partner Requirement

Consolidators must have written and verifiable processes for the screening and selection of business partners, including foreign consolidators, customers, contractors, carriers, and vendors. Ensure that contracted service provider companies who provide transportation, cargo handling, and security services commit to CTPAT security procedures guidelines. Periodically review the performance of the service providers to detect weakness, or potential weakness, in security.

Security procedures

- **Point of Origin**

  CTPAT Consolidators must ensure that business partners develop security processes and procedures consistent with the CTPAT security procedures guidelines to enhance the integrity of the shipment at point of origin. Periodic reviews of business partners' processes and facilities should be conducted based on risk and should maintain the security standards required by the Consolidator.

• Participation/Certification in Your National Customs Administration's SupplyChain Security Program.

Current or prospective business partners who have obtained a certification in a supply chain security program administered by their national Customs Administration should be required to indicate their status of participation to the CTPAT Consolidator.

• Service Provider Screening and Selection Procedures

The CTPAT Consolidator should have documented service provider screening and selection procedures to screen the contracted service provider for validity, financial soundness, ability to meet contractual security requirements, and the ability to identify and correct security deficiencies as needed. Service Provider procedures should use a riskbased process as determined by an internal management team.

• Customer Screening Procedures

The CTPAT Consolidator should have documented procedures to screen prospective customers for validity, financial soundness, the ability to meet contractual security requirements, and the ability to identify and correct security deficiencies as needed. Customer screening procedures should use a risk-based process as determined by an internal management team.

Container Security

Container and trailer integrity must be maintained to protect against the introduction of unauthorized material and/or persons. At the point-of-stuffing, procedures must be in place to properly seal and maintain the integrity of the shipping containers and trailers. A high security seal must be affixed to all loaded containers and trailers bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standard for high security seals.

- **Container Inspection**

Procedures must be in place to verify the physical integrity of a shipping-container's structure prior to stuffing, to include the reliability of the locking mechanisms of the doors. A seven-point inspection process is recommended for all containers:

1. Front wall
2. Left side
3. Right side
4. Ceiling/Roof
5. Inside/Outside doors
6. Outside/Undercarriage
7. Floor

- **Container Seals**

Written procedures must stipulate how seals are to be controlled and affixed to loaded containers. Procedures must be in place for recognizing and reporting compromised seals and/or containers to U.S. Customs and Border Protection, or the appropriate foreign authority. Only designated employees should distribute container seals for integrity purposes.

- **Container Storage**
  Containers must be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting and neutralizing unauthorized entry into containers or container storage areas.

Physical Access Controls

Access controls prevent unauthorized entry to facilities, maintain control of employees and visitors and protect company assets. Access controls must include the positive identification of all employees, visitors, and vendors at all points of entry.

• **Employees**

An employee identification system must be in place for positive identification and access control purposes. Employees should be given access only to those secure areas needed for the performance of their duties. Company management or security personnel must adequately control the issuance and removal of employee, visitor, and vendor identification badges. Procedures for the issuance, removal, and changing of access devices (e.g. keys, key cards, etc.) must be documented.

• **Visitors Controls**
Visitors must present photo identification for documentation purposes upon arrival. All visitors should be escorted and visibly display temporary identification.

• **Deliveries (including mail)**
Proper vendor ID and/or photo identification must be presented for documentation purposes by all vendors. Arriving packages and mail should be periodically screened before being disseminated.

• **Challenging and Removing Unauthorized Persons**
Procedures must be in place to identify, challenge, and address unauthorized/unidentified persons.

Personnel Security

Processes must be in place to screen prospective employees and to periodically check current employees. Maintain a current permanent employee list (foreign and domestic), which includes the name, date of birth, national identification number or social security number, and position held, and submit such information to CBP upon written request, to the extent permitted by law.

- **Pre-Employment Verification**
  Application information, such as employment history and references must be verified prior to employment.

- **Background checks / investigations**
  Consistent with foreign, federal, state, and local regulations, background checks, and investigations should be conducted for prospective employees. Periodic checks and reinvestigations should be performed based on cause and/or the sensitivity of the employee's position.

- **Personnel Termination Procedures**
  Companies must have procedures in place to remove identification, as well as facility and system access for terminated employees.

Procedural Security

Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain.

- **Documentation Processing**
  Procedures must be in place to ensure that all documentation used in the movement of merchandise/cargo is legible, complete, accurate, and protected against the exchange, loss, or introduction of erroneous information. Documentation control must include safeguarding computer access and information.

- **Manifesting Procedures**
  To help ensure the integrity of cargo received from abroad, procedures must be in place to ensure that information received from business partners is reported accurately and in a timely manner.

- **Shipping & Receiving**
  Arriving cargo should be reconciled against information on the cargo manifest. The cargo should be accurately described, weighed, labeled, marked, counted, and verified. Departing cargo should be checked against purchase or delivery orders. Drivers delivering or receiving cargo must be positively identified before cargo is received or released.

- **Cargo Discrepancies**
  All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. CBP and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected.

Security Training and Threat Awareness

A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by terrorists at each point in the supply chain. Employees must be made aware of the procedures the company has in place to address a situation and how to report it. Additional training should be provided to employees in the shipping and receiving areas, as well as those receiving and opening mail.

Additionally, specific training should be offered to assist employees in maintaining cargo integrity, recognizing internal conspiracies, and protecting access controls. These programs should offer incentives for active employee participation.

Physical Security

Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access. Consolidators should incorporate the following CTPAT physical security guidelines throughout their supply chains as applicable:

- **Fencing**
  Perimeter fencing should enclose the areas around cargo handling and storage facilities. Interior fencing within a cargo handling structure should be used to segregate domestic, international, high value, and hazardous cargo. All fencing must be regularly inspected for integrity and damage.

- **Gates Gate Houses**
  Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety.

- **Parking**
  Private passenger vehicles should be prohibited from parking in, or adjacent to, cargo handling and storage areas.

- **Building Structure**
  Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.

- **Locking Devices and Key Controls**
  All external and internal windows, gates, and fences must be secured with locking devices. Management or security personnel must control the issuance of all locks and keys.

- **Lighting**
  Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, cargo handling, storage areas, fence lines, and parking areas.

- **Alarms Systems & Video Surveillance Cameras**
  Alarm systems and video surveillance cameras should be used to monitor premises and prevent unauthorized access to cargo handling and storage areas.

Cybersecurity

Consolidators and their partners 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 below. Information Technology (IT) integrity must be maintained at all times to protect data from unauthorized access or manipulation.

- **Network Protection**
  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.

- **Testing**
  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.

- **User Access**
  User access must be restricted based on job description or assigned duties. Individuals with access to Information Technology (IT) systems must use individually assigned accounts. 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.

- **Accountability & Identification of Abuse**
  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

- **Password Protection**
  Automated systems must use individually assigned accounts that require a periodic change of password. IT security policies, procedures, and standards must be in place and training provided to employees. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication and user access to IT systems must be

safeguarded. Passwords and/or passphrases must be changed as soon as possible if there is evidence of compromise or reasonable suspicion of a compromise exists.

• **VPNs**

Members that allow their users to remotely connect to a network must employ secure technologies such as virtual private networks (VPNs) or multi-factor authentication (MFA) 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.

• **Data**

Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format.

Trade-Based Money Laundering

Trade-Based Money Laundering occurs when criminals use the international trade system to disguise illicit proceeds by altering Customs and banking paperwork to make transactions appear legitimate. These proceeds are then used to finance additional criminal activity, which may include funding terrorist activities or organizations.

CTPAT Members and their business partners 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 criminal funding as there is a marked overlap between the two. Specialized training should be provided annually to personnel who may be able to identify the warning indicators of TradeBased Money Laundering and Terrorism Financing (examples of personnel who should receive this training include those responsible for trade compliance, security, procurement, finance, shipping, and receiving).

For further information, please consult the document CTPAT's Warning Indicators for TradeBased Money Laundering and Terrorism Financing Activities on the Tricar Sales website or the website of the U.S. Customs and Border Patrol CTPAT program.

The following are examples of some of the vetting elements that can help determine if a company is legitimate:

- Verifying the company's business address and how long they have been at that address.
- Conducting research on the internet on both the company and its principals.
- Checking business references.
- Requesting a credit report.

Upper Management Responsibility

The role of a company's upper management in CTPAT is to provide support and oversight to ensure the creation and maintenance of the company's Supply Chain Security Program. To this end, the designated company CTPAT administrator, head of security, or security coordinator should provide regular updates regarding the progress or outcomes of any audits, exercises, or validations to upper management.

To promote a culture of security, a letter of commitment to supply chain security (and/or the CTPAT program) should be signed by a senior company official and displayed in appropriate company locations.

Wood Packaging Materials, Pallets (Agricultural Procedures)

Visible pest contamination is to include compliance with Wood Packaging Materials (WPM) regulations. Measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15). This is a firm requirement of CTPAT as visible pest prevention measures must be adhered to throughout the supply chain.

Note to Consolidators and Carrier-Forwarders:

Please send the *Highway Carrier* guidelines below to your trucking companies in order to request their fulfilment of the guidelines, if they are not already doing so.

Note we have also included guidelines for the industrial sectors: Sea, Air, Rail Carriers and NVOCCs These may be sent to those companies as appropriate.

Highway Carriers
CTPAT Security Criteria:

The supply chain for highway carriers for CTPAT purposes is defined from point of origin from the yard or where the tractors and trailers are stored, through pickup at the manufacturer, supplier or vendor, through to the point of distribution - and recognizes the diverse business models CTPAT members employ.

These minimum-security criteria are designed for highway carriers to optimize supply chain performance, to mitigate the risk of loss, theft, and contraband smuggling that could potentially introduce dangerous elements into the global supply chain.

On a quarterly basis, or as circumstances dictate, highway carriers should assess their vulnerability to risk and should prescribe security measures to strengthen or adjust their security posture to prevent security breaches and internal conspiracies. The determination and scope of criminal elements targeting world commerce through internal conspiracies requires companies -- and in particular, highway carriers -- to elevate their security practices.

CTPAT recognizes the complexity of international supply chains and security practices and endorses the. application and implementation of security measures based upon risk. Therefore, the program allows for flexibility and the customization of security plans based on the member's business model. Appropriate security measures, as listed throughout this document, must be implemented and maintained.

Business Partner Requirements

Highway carriers must have written and verifiable processes for screening business partners, including agents, sub-contracted carriers, service providers and new customers for financial soundness issues. Security indicators, such as business references and professional associations, should be included.

Security Procedures

- Written procedures must exist for screening business partners which identify specific factors or practices, the presence of which would trigger additional scrutiny by the highway carrier.
- For those business partners eligible for CTPAT certification (importers, ports, terminals, brokers, consolidators, carrier-forwarders, etc.) the highway carrier must have documentation indicating whether these business partners are, or are not, CTPAT certified. Non-CTPAT business partners may be subject to additional scrutiny by the highway carrier.
- Highway carriers should ensure that contract service providers commit to CTPAT security recommendations through contractual agreements. For U.S. bound shipments, CTPAT highway carriers that subcontract transportation services to other highway carriers must use other CTPAT-approved highway carriers or carriers under direct control of the certified CTPAT carrier through a written contract.
- Likewise, current or prospective business partners who have certification in a supply-chain security program being administered by a foreign Customs Administration should be required to indicate their status of participation to the highway carrier.

As highway carriers have the ultimate responsibility for all cargo loaded aboard their trailer or conveyance, they must communicate the importance of supply chain security and maintaining chain of custody as fundamental aspects to any company security policy.

Conveyance Security

Conveyance (tractor and trailer) integrity procedures must be maintained to protect against the introduction of unauthorized personnel and material.

Conveyance Inspection Procedures

• Using a checklist, drivers should be trained to inspect their conveyances for natural or hidden compartments. Training in searches should part of the company's on-the-job training.
• Inspections must be systematic and completed upon entering and departing from the truck yard, and at the last point of loading prior to reaching the U.S. border.
• To counter internal conspiracies, supervisory personnel or a security manager -- held accountable to senior management for security -- should search the conveyance after the driver has conducted a search. These searches should be random, documented, based on risk, and conducted at the truck yard, after the truck has been loaded and is en route to the U.S. border.
• Written procedures must exist which identify specific factors or practices which may deem a shipment from a certain shipper to be of greater risk.
• The following systematic practices should be considered when conducting training on conveyances. Highway carriers must visually inspect all empty trailers, to include the interior of the trailer, at the truck yard and at the point of loading, if possible. The following inspection process is recommended for all trailers and tractors:

1. Tractors:

• Bumper/tires/rims
• Doors/tool compartments • Battery box
• Air breather
• Fuel tanks
• Interior cab compartments/sleeper
• Roof

2. Trailers:

• Fifth wheel area - check natural compartment/skid plate
• Exterior - front/sides
• Rear - bumper/doors
• Front wall
• Left side
• Right side
• Floor
• Ceiling/Roof
• Inside/outside doors
• Outside/Undercarriage

Trailer Security

• For all trailers in the highway carrier's custody, trailer integrity must be maintained to protect against the introduction of unauthorized material and/or persons at all times.

• it is recognized that even though a carrier may not "exercise control" over the loading of trailers and the contents of the cargo, highway carriers must be vigilant to help ensure that the merchandise is legitimate, and that there is no loading of contraband at the loading dock/manufacturing facility. The highway carrier must ensure that while in transit to the border, no loading of contraband has occurred, even in regard to unforeseen vehicle stops.

• Trailers must be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting and neutralizing unauthorized entry into trailers, tractors, or storage areas.

• The carrier must notify U.S. Customs and Border Protection of any structural changes, such as a hidden compartment, discovered in trailers, tractors, or other rolling-stock equipment that crosses the border. Notification should be made immediately to CBP, and in advance of the conveyance crossing the border. Notifications can be telephonically made to CBP's Anti-Terrorism Contraband Enforcement Team (ATCET) at the port.

Container Security

When transporting a container or trailer for a CTPAT importer, a high security seal that meets or exceeds the current PAS ISO 17712 standards for high security seals must be used.

Conveyance Tracking and Monitoring Procedures

• Highway Carriers must ensure that conveyance and trailer integrity is maintained while the conveyance is transporting cargo en route to the U.S. border by using a tracking and monitoring activity log, or equivalent technology. If driver logs are used, they must reflect that trailer integrity was verified.

• Predetermined routes should be identified, and procedures should consist of random route checks, along with documenting and verifying the length of time between the loading point/trailer pickup, the U.S. border, and the delivery destinations during peak and non-peak times. Drivers should notify the dispatcher of any route delays due to weather, traffic, and/or rerouting.

• Highway Carrier management must perform a documented, periodic, and unannounced verification process to ensure the logs are maintained, and that conveyance tracking and monitoring procedures are being followed and enforced.

• During Department of Transportation Inspections (DOT) or other physical inspections on the conveyance as required by state, local, or federal law, drivers must report and document any anomalies or unusual structural modifications found on the conveyance. In addition, Highway Carrier management should perform a documented, periodic, and unannounced verification process to ensure the logs are maintained, and that conveyance tracking and monitoring procedures are being followed and enforced.

Trailer Seals

• The sealing of trailers, to include continuous seal integrity, is a crucial element of a secure supply chain, and remains a critical part of a carrier's commitment to CTPAT. A high security seal must be affixed to all loaded trailers if bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standards for high security seals.

• Based on risk, a high security barrier bolt seal may be applied to the door handle and/or a cable seal must be applied to the two vertical bars on the trailer doors. • Clearly defined written

procedures must stipulate how seals in the highway carrier's possession are to be controlled during transit. These written procedures should be briefed to all drivers and there should be a mechanism to ensure that these procedures are understood and are being followed. These procedures must include:

− Verifying that the seal is intact, or whether it exhibits evidence of tampering along the route,
− Properly documenting the original and second seal numbers.
− Verify that the seal number and location of the seal are the same as stated by the shipper on the shipping documents.
− If the seal is removed in-transit to the border, even by government officials, a second seal must be placed on the trailer, and the seal change must be documented.
− The driver must immediately notify the dispatcher that the seal was broken, by whom, and the number of the second seal that is placed on the trailer.
− The carrier must make immediate notification to the shipper, the customs broker and/or the importer of the placement of the second seal.

Less-than Truck Load (LTL)

• LTL carriers must use a high security padlock or similarly appropriate locking device when picking up local freight in an international LTL environment, LTL carriers must ensure strict controls to limit the access to keys or combinations that can open these padlocks.
• After the freight from the pickup and delivery run is sorted, consolidated, and loaded onto a line haul carrier destined to cross the border into the U.S., the trailer must be sealed with a high security seal which meets or exceeds the current PAS ISO 17712 standard for high security seals.
• In LTL or Pickup and Delivery (P&D) operations that do not use consolidation hubs to sort or consolidate freight prior to crossing the U.S. border, the importer and/or highway carrier must use ISO 17712 high security seals for the trailer at each stop, and to cross the border.
• Written procedures must be established to record the change in seals, as well as stipulate how the seals are controlled and distributed, and how discrepancies are noted and reported. These written procedures should be maintained at the terminal/local level.
• in the LTL and non-LTL environment, procedures should also exist for recognizing and reporting compromised seals and/or trailers to U.S. Customs and Border Protection or the appropriate foreign authority.

Physical Access Controls

Access controls prevent unauthorized entry to trucks, trailers, and facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, service providers, and vendors at all points of entry. Employees and service providers should have access only to those areas of a facility where they have legitimate business.

• **Employees**
An employee identification system must be in place for positive identification and access control purposes. Employees should be given access only to those secure areas needed for the performance of their duties. Company management or security personnel must adequately control the issuance and removal of employee, visitor, and vendor identification badges. Procedures for

the issuance, removal, and changing of access devices (e.g. keys, key cards, etc.) must be documented.

• **Visitors/Vendors/Service Providers**
Visitors, vendors, and service providers must present photo identification for documentation purposes upon arrival, and a log must be maintained. All visitors and service providers should visibly display temporary identification.

• **Challenging and Removing Unauthorized Persons**
Procedures must be in place to identify, challenge, and address unauthorized/unidentified persons.

Personnel Security

Written and verifiable processes must be in place to screen prospective employees and to periodically check current employees.

• Pre-Employment Verification Application information, such as employment history and references, must be verified prior to employment.

• Background Checks/Investigations Consistent with foreign, federal, state, and local regulations, background checks and investigations should be conducted for prospective employees. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position. • Personnel Termination Procedures Companies must have procedures in place to remove identification, as well as facility, and system access for terminated employees.

Procedural Security

Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain. Procedures must be in place to prevent, unmanifested material and unauthorized personnel from gaining access to the conveyance, including concealment in trailers.
Security procedures should be implemented that restrict access to the conveyance and prevent the lading of contraband while en-route from facilities in international locations to the United States.

Procedures must be in place to record and immediately report all anomalies regarding truck drivers to U.S. Customs and Border Protection. If local, federal, or state laws and union rules permit, random screening of truck driver luggage and personal effects should be done.

• **Documentation Processing**
Procedures must be in place to ensure that all information used in the clearance of merchandise/cargo, is legible, complete, accurate, and protected against the exchange, loss, or introduction of erroneous information. Measures, such as using a locked filing cabinet, should also be taken to secure the storage of unused forms, including manifests, to prevent unauthorized use of such documentation

• Document Review Personnel should be trained to review manifests and other documents in order to identify or recognize suspicious cargo shipments that:

- Originate from, or are destined to, unusual locations.
- Are paid by cash or certified check.
- Have unusual routing methods.
- Exhibit unusual shipping/receiving practices.
- Provide vague, generalized, or poor information.
- All instances of a suspicious cargo shipment should be reported immediately to the nearest U.S. Customs and Border Protection port-of-entry.

Bill of Lading/Manifesting Procedures

Bill of lading information filed with CBP should show the first foreign location/facility where the highway carrier takes possession of the cargo destined for the United States. Additionally, to help ensure the integrity of cargo received from abroad, procedures must be in place to ensure that information received from business partners is reported accurately and in a timely manner.

• Cargo

Cargo must be properly marked and manifested to include accurate weight and piece count. Customs and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected.

Physical Security

Procedures must be in place to prevent, unmanifested material and unauthorized personnel from gaining access to a conveyance, including concealment in trailers. Cargo handling and storage facilities, trailer yards, etc., must have physical barriers and deterrents that guard against unauthorized access. Highway carriers should incorporate the following CTPAT physical security criteria throughout their supply chains as applicable:

• Fencing

Perimeter fencing should enclose the entire truck yard or terminal, especially areas where tractors, trailers, and other rolling stock are parked or stored. All fencing must be regularly inspected for integrity and damage.

• Gates and Gate Houses

Gates through which all vehicles and/or personnel enter or exit must be manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety.

• Parking

Private passenger vehicles must be prohibited from parking in close proximity to parking and storage areas for tractors, trailers, and other rolling stock that crosses the international border.

• Building Structure

Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.

- **Locking Devices and Key Controls**

All external and internal windows, gates, and fences must be secured with locking devices. Management or security personnel must control the issuance of all locks and keys, to include the locks and keys for tractors, When parked in the yard, doors to tractors should be locked and the windows closed to prevent unauthorized access.

- **Lighting**

Adequate lighting must be provided inside and outside the facility, including the following areas: entrances and exits, parking, or storage areas for tractors, trailers, rolling stock, and fences.

- **Alarms Systems & Video Surveillance Cameras**

Alarm systems and video surveillance cameras should be used to monitor the premises and prevent unauthorized access to vessels, and cargo handling and storage areas, based on risk.

Security Training and Threat Awareness

A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by drug smugglers and terrorists at each point in the supply chain. Employees must be made aware of the procedures the highway carrier has in place to address a situation and how to report it.

Additionally, specific training should be offered to assist employees in maintaining trailer and tractor integrity, recognizing internal conspiracies, and protecting access controls. These programs should offer incentives for active employee participation.

Cybersecurity

A system must be in place to identify the abuse of information Technology (IT) including improper access, tampering, or the altering of business data. All system violators must be to appropriate disciplinary action.

- **Network Systems**

Network systems must be regularly tested for the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.

- **Sharing Information On Cybersecurity Threats**

A carrier's IT policies should address how the carrier shares information on cybersecurity threats with the government and other business partners.

- **Identifying Abuse**

Systems 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.

- **Unauthorized Access**

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

- **Annual Review C**

ybersecurity policies and procedures must be reviewed annually.

- **User access**

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.

- **Individually Assigned Accounts**

Individuals with access to Information Technology (IT) systems must use individually assigned accounts. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication, and user access to IT systems must be safeguarded.

- **Passwords**

Passwords and/or passphrases must be regularly changed, but also changed as soon as possible if there is evidence of compromise or reasonable suspicion of a compromise exists. As well, passwords should be complex.

- **VPNs**

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.

- **Employee Devices**

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.

Trade-Based Money Laundering

Trade-Based Money Laundering occurs when criminals use the international trade system to disguise illicit proceeds by altering Customs and banking paperwork to make transactions appear legitimate. These proceeds are then used to finance additional criminal activity, which may include funding terrorist activities or organizations.

CTPAT Members and their business partners 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 criminal funding as there is a marked overlap between the two. Specialized training should be provided annually to personnel who may be able to identify the warning indicators of Trade-Based Money Laundering and Terrorism Financing (examples of personnel who should receive this training include those responsible for trade compliance, security, procurement, finance, shipping, and receiving).

For further information, please consult the document CTPAT's Warning Indicators for Trade-Based Money Laundering and Terrorism Financing Activities, as found on the internet by the U.S. Customs and Border Patrol CTPAT program website.

The following are examples of some of the vetting elements that can help determine if a company is legitimate:

- Verifying the company's business address and how long they have been at that address.
- Conducting research on the internet on both the company and its principals.
- Checking business references.
- Requesting a credit report.

Upper Management Responsibility

The role of a company's upper management in CTPAT is to provide support and oversight to ensure the creation and maintenance of the company's Supply Chain Security Program. To this end, the designated company CTPAT administrator, head of security, or security coordinator should provide regular updates regarding the progress or outcomes of any audits, exercises, or validations to upper management.

To promote a culture of security, a letter of commitment to supply chain security (and/or the CTPAT program) should be signed by a senior company official and displayed in appropriate company locations.

Wood Packaging Materials, Pallets (Agricultural Procedures)

Visible pest contamination is to include compliance with Wood Packaging Materials (WPM) regulations. Measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15). This is a firm requirement of CTPAT as visible pest prevention measures must be adhered to throughout the supply chain.

Sea Carriers
CTPAT Security Procedures Guidelines

Sea carriers must conduct a comprehensive assessment of their security practices based upon the following CTPAT minimum-security criteria. Where a sea carrier does not control a specific element of the cargo transportation service it has contracted to provide, such as marine terminal operator or a time chartered vessel with whom it has contracted, the sea carrier must work with these business partners to ensure that pertinent security measures are in place and adhered to. The sea carrier is responsible for exercising prudent oversight for all cargo loaded on board its vessel, pursuant to applicable law and regulations, and the terms of this program.

CTPAT recognizes the complexity of international supply chains and security practices and endorses the application and implementation of security measures based upon risk. Therefore, the program allows for flexibility and the customization of security plans based on the member's business model. Security measures, as listed throughout this document, must be implemented and maintained as appropriate to the carrier's business model and risk understanding. CBP's CTPAT validation process shall include a review of the carrier's assessment and program.

CTPAT recognizes that sea carriers are already subject to defined security mandates created under the International Ship and Port Security Code (ISPS) and the Maritime Transportation Security Act (MTSA). It is not the intention of CTPAT to duplicate these vessel and facility security requirements, rather, CTPAT seeks to build upon the ISPS and MTSA foundation and require additional security measures and practices which enhance the overall security throughout the international supply chain.

ISPS and MTSA compliance are a prerequisite for CTPAT sea carrier membership, and only vessels in compliance with the applicable ISPS code requirements may be used by CTPAT members. Marine terminals operated by CTPAT members must also comply with ISPS code requirements. The Physical Access Controls and Physical Security provisions of these criteria are satisfied for ISPS regulated vessels and port facilities by those vessels' or facilities' compliance with the ISPS Code and Coast Guard regulations.

Business Partner Requirements

Sea carriers must have written and verifiable procedures for the screening of carrier's agents and service providers contracted to provide transportation services for the carrier. Sea carriers must also have screening procedures for new customers, beyond financial soundness issues, to include indicators of whether the customer appears to be a legitimate business and/or poses a security risk. Sea carriers shall also have procedures to review their customer's requests that could affect the safety of vessels or cargo or otherwise raise significant security questions, including unusual customer demands, such as specific stowage placement aboard the vessel (beyond a request for below deck or on deck stowage). ;

- **Security procedures**

  Sea carriers must have written or web-based procedures for screening new customers to whom they issue bills of lading, which identify specific factors or practices, the presence of which would trigger additional scrutiny by the sea carrier, up to, and including, a detailed physical inspection of the exterior of the suspect customer's container prior to loading onto the vessel. These procedures may also include a referral to CBP or other competent authorities for further review. CBP will work

in partnership with the sea carriers to identify specific information regarding what factors, practices, or risks are relevant.

Sea carriers should ensure that contract vessel services providers commit to CTPAT security recommendations. Periodic reviews of the security commitments of the service providers should be conducted.

Container Security

For all containers in the sea carrier's custody, container integrity must be maintained to protect against the introduction of unauthorized material and/or persons. Sea carriers must have procedures in place to maintain the integrity of the shipping containers while in their custody. A high security seal must be affixed to all loaded containers bound for the U.S. All seals used or distributed by the sea carrier must meet or exceed the current PAS ISO 17712 standards for high security seals.

Sea carriers and/or their marine terminal operators must have processes in place to comply with seal verification rules and seal anomaly reporting requirements promulgated and mandated by the U.S. government.

- **Container Inspection**

The requirement to inspect all containers prior to stuffing (to include the reliability of the locking mechanisms of doors) is placed upon the importers through the CTPAT Minimum Security Criteria for Importers dated March 25, 2005. Sea carriers must visually inspect all U.S.-bound empty containers, to include the interior of the container, at the foreign port of lading.

- **Container Seals**

Written procedures must stipulate how seals in the sea carrier's possession are to be controlled. Procedures should also exist for recognizing and reporting compromised seals and/or containers to US Customs and Border Protection or the appropriate foreign authority consistent with the seal anomaly reporting requirements promulgated and mandated by the U.S. government.

- **Container Storage**

The sea carrier must store containers in their custody in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting, unauthorized entry into containers or container storage areas to appropriate local law enforcement officials.

Physical Access Controls

The sea carrier shall establish access controls to prevent unauthorized entry to its vessels and cargo facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, service providers, government officials, and vendors at all restricted access points of entry. Shore employees and service providers should have access only to those areas of the vessel where they have legitimate business. Vessel and facility access controls are governed by the International Ship and Port Security Code and MTSA. The Physical Access Control provisions of these criteria are satisfied for ISPS regulated vessels and port facilities by those vessels' or facilities' compliance with the ISPS Code and MTSA regulations.

• **Boarding and Disembarking of Vessels**
Consistent with the vessel's ISPS security plan, all crew, employees, vendors, and visitors may be subject to a search when boarding or disembarking vessels. A vessel visitor log must be maintained, and a temporary visitor pass must be issued as required by the vessel's security plan. All crewmembers, employees, vendors, and visitors, including government officials, must display proper identification as required by the applicable ISPS/MTSA security plan.

• **Employees**
An employee identification system must be in place for positive identification and access control purposes. Employees should be given access only to those secure areas needed for the performance of their duties. Company management or security personnel must adequately control the issuance and removal of employee, visitor, and vendor identification badges. Procedures for the issuance, removal, and changing of access devices (e.g. keys, key cards, etc.) must be documented.

• **Visitors/Vendors/Service Providers**
Visitors, vendors, government officials, and service providers must present photo identification for documentation purposes upon arrival at carrier's vessels or cargo facilities, and a visitor log must be maintained. Measures described by the approved ISPS/MTSA security plan addressing the escort of visitors and service providers, including, when appropriate, the use of temporary identification, will be followed.

• **Challenging and Removing Unauthorized Persons**
Procedures must be in place to identify, challenge, and address unauthorized/unidentified persons.

Personnel Security

In compliance with applicable laws and regulations for that location, written and verifiable processes must be in place to screen prospective employees and to check current employees periodically.

• **Pre-Employment Verification**
Application information, such as employment history and references, must be verified prior to employment.
• **Background checks / investigations**
Depending on the sensitivity of the position, background checks and investigations shall be conducted for prospective employees as appropriate, and as required by foreign, federal, state, and local regulations. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.
• **Personnel Termination Procedures**
Companies must have procedures in place to remove identification, as well as facility, and system access, for terminated employees.
• **Crewmen Control - Deserter/Absconder Risk**
CBP will work with the U.S. Coast Guard and sea carriers to identify specific factors which may indicate when a crewman poses a potential risk of desertion/absconding. When such factors are identified and provided to the carriers, the carrier shall provide this information to its vessel masters and to the vessels under charter to the carrier, and such vessels shall establish procedures to address the potential risk of desertion/absconding. Added security measures appropriate to the risk should be employed upon arrival into the U.S. port/territories.

- **Deserter/Absconder Notifications**

Vessel masters must account for all crewmen prior to the vessel's departure from a U.S. port. If the vessel master discovers that a crewman has deserted or absconded, the vessel master must report this finding, by the most practical means, to CBP immediately upon discovery, and prior to the vessel's departure.

Procedural Security

Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo. Consistent with the carrier's ISPS Code security plan, procedures must be in place to prevent unauthorized personnel from gaining access to the vessel. In those geographic areas where risk assessments warrant checking containers for human concealment in containers, procedures should be designed to address the particular, identified risk at the load port or the particular port facility. CBP will inform the sea carriers when it is aware of a high risk of human concealment or stowaways at particular ports or geographic regions. Documented procedures must also include pre-departure vessel security sweeps for stowaways at the foreign load port, and during normal watch activity while en route to the United States as warranted by risk conditions at the foreign load port.

- **Passenger and Crew**

Sea carriers must ensure compliance with the U.S. Coast Guard Notice of Arrival and Departure requirements so that accurate and advanced transmission of data associated with international passengers and crew is provided to the U.S. government and CBP in a timely manner.

- **Bill of Lading / Manifesting Procedures**

Procedures must be in place to ensure that the information in the carrier's cargo manifest accurately reflects the information provided to the carrier by the shipper or its agent and is filed with CBP in a timely manner. Documentation control must include safeguarding computer access and information. Bill of lading information filed with CBP should show the first foreign port (place) where the sea carrier takes possession of the cargo destined for the United States.

- **BAPLIEs**

At the request of CBP, sea carriers will provide a requested BAPLIE and/or stowage plan, in a format readily available. Such requests will be made on a voyage-specific basis when CBP requires additional voyage information and will be honored by the sea carrier in a timely manner. CBP recognizes that these are not regulated documents and that the data included may not always match the manifest filing.

- **Cargo**

Customs and/or other appropriate law enforcement agencies must be notified if illegal or highly suspicious activities are detected.

Security Training and Awareness

A security awareness program should be established and maintained by the carrier to recognize and foster awareness of security vulnerabilities to vessels and maritime cargo. Employees must be made aware of the procedures the sea carrier has in place to report a security concern or incident.

Additionally, specific training should be offered to assist employees in maintaining vessel and cargo integrity, recognizing internal conspiracies, and protecting access controls.

Physical Security Carriers shall establish written and verifiable procedures to prevent unauthorized personnel from gaining access to its vessels, including concealment in containers, and to prevent tampering with cargo conveyances while they are in the carrier's custody. Such measures are covered by a vessel's and a port facility's ISPS security plan. Physical Security provisions of these criteria are satisfied for ISPS

regulated vessels and port facilities by those vessels' or facilities' compliance with the ISPS Code and MTSA regulations. Non-ISPS Code regulated cargo handling and storage facilities, and container yards operated by the carrier in domestic and foreign locations, must have physical barriers and deterrents that guard against unauthorized access. Sea carriers should incorporate the following CTPAT physical security criteria as applicable:

- **Fencing**
  Perimeter fencing should enclose the areas around cargo handling and storage facilities, container yards, an terminals. All fencing must be inspected regularly for integrity and damage.

- **Gates and Gate Houses**
  Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored and secure when not in use.

- **Parking**
  Private passenger vehicles should be prohibited from parking in, or adjacent to, cargo handling and storage area, and vessels.

- **Building Structure**
  Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.

- **Locking Devices and Key Controls**
  All external and internal windows, gates, and fences must be secured with locking devices. Management or security personnel must control the issuance of all locks and keys.

- **Lighting**
  Adequate lighting must be provided inside and outside the facility, including the following areas: entrances and exits, cargo handling and storage areas, fence lines, and parking areas. While at port, the pier and waterside of the vessel must be adequately illuminated.

- **Alarms Systems & Video Surveillance Cameras**
  At those locations determined appropriate by the carrier's risk assessment, alarm systems and video surveillance cameras should be used to monitor premises and prevent unauthorized access to vessels, as well as cargo handling and storage areas.

Cybersecurity
A system must be in place to identify the abuse of Information Technology (IT) including improper access, tampering, or the altering of business data. All system violators must be to appropriate disciplinary action.

- **Network Systems**
  Network systems must be regularly tested for the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.

- **Sharing Information On Cybersecurity Threats**
  Company IT policies should address how the company shares information on cybersecurity threats with the government and other business partners.

- **Identifying Abuse**
Systems 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.

- **Unauthorized Access**
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

- **Annual Review**
Cybersecurity policies and procedures must be reviewed annually.

- **User access**
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.

- **Individually Assigned Accounts**
Individuals with access to Information Technology (IT) systems must use individually assigned accounts. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication, and user access to IT systems must be safeguarded.

- **Passwords**
Passwords and/or passphrases must be regularly changed, but also changed as soon as possible if there is evidence of compromise or reasonable suspicion of a compromise exists. As well, passwords should be complex.

- **VPNs**
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.

- **Employee Devices**
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.

Security Assessment, Response and Improvement

Carriers and CBP have a mutual interest in security assessments and improvements, and recognize that specific, implemented security procedures may be found in the future to have weaknesses or be subject to circumvention. When a security shortcoming or security incident is identified, the carrier and CBP officials will meet in an effort to ascertain what led to the breakdown, and to formulate mutually agreed remedial measures.

If CBP determines that the security incident raises substantial concerns or a security weakness requires substantial remediation, CBP headquarters officials will meet with the carrier's senior management to discuss such concerns, and to identify appropriate remedial measures to be taken.

A system must be in place to identify the abuse of IT, including improper access, tampering, or the altering of business data. All system violators must be to appropriate disciplinary action

Trade-Based Money Laundering

Trade-Based Money Laundering occurs when criminals use the international trade system to disguise illicit proceeds by altering Customs and banking paperwork to make transactions appear legitimate. These proceeds are then used to finance additional criminal activity, which may include funding terrorist activities or organizations.

CTPAT Members and their business partners 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 criminal funding as there is a marked overlap between the two. Specialized training should be provided annually to personnel who may be able to identify the warning indicators of TradeBased Money Laundering and Terrorism Financing (examples of personnel who should receive this training include those responsible for trade compliance, security, procurement, finance, shipping, and receiving).

For further information, please consult the document CTPAT's Warning Indicators for TradeBased Money Laundering and Terrorism Financing Activities, as found on the Tricar Sales web site or the website of the U.S. Customs and Border Patrol CTPAT program.

The following are examples of some of the vetting elements that can help determine if a company is legitimate:

- Verifying the company's business address and how long they have been at that address.
- Conducting research on the internet on both the company and its principals.
- Checking business references.
- Requesting a credit report.

Upper Management Responsibility

The role of a company's upper management in CTPAT is to provide support and oversight to ensure the creation and maintenance of the company's Supply Chain Security Program. To this end, the designated company CTPAT administrator, head of security, or security coordinator should provide regular updates regarding the progress or outcomes of any audits, exercises, or validations to upper management.

To promote a culture of security, a letter of commitment to supply chain security (and/or the CTPAT program) should be signed by a senior company official and displayed in appropriate company locations.

Wood Packaging Materials, Pallets (Agricultural Procedures)

Visible pest contamination is to include compliance with Wood Packaging Materials (WPM) regulations. Measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15). This is a firm requirement of CTPAT as visible pest prevention measures must be adhered to throughout the supply chain.

-- continued below --

Air Carriers
CTPAT Security Procedures Guidelines

Air carriers must conduct a comprehensive assessment of their security practices based upon the following CTPAT minimum-security criteria. Where an air carrier does not control a specific element of the cargo transportation service it has contracted to provide, such as an airport terminal, direct handling of cargo containers or Unit Load Device (ULD), or processes subject to these criteria, the air carrier must work with these business partners to ensure that pertinent security measures are in place and adhered to.

The air carrier is responsible for exercising prudent oversight for all cargo loaded on board its aircraft, pursuant to applicable laws and regulations and the terms of this program. CTPAT recognizes the complexity of international supply chains and security practices, and endorses the application and implementation of security measures based upon risk.1 Therefore, the program allows for flexibility and the customization of security plans based on the member's business model. Appropriate security measures/as listed throughout this document, must be implemented and maintained.

CTPAT also acknowledges that air carriers are already subject to defined security mandates created through public laws and regulations, such as the Aviation and Transportation Security Act (PL 107-71). It is not the intention of CTPAT to duplicate these requirements, rather, CTPAT seeks to build upon established foundations and require additional security measures and practices which enhance the overall security throughout the international supply chain. The CTPAT program is therefore working closely with the Transportation Security Administration to establish connectivity between the CTPAT validation process and the TSA know shipper program. The international supply chain for CTPAT purposes is defined from point of origin (manufacturer/supplier/vendor) through point of distribution - and recognizes the diverse business models CTPAT members employ.

Certified CTPAT air carriers must cooperate fully with CBP and other Department of Homeland Security law enforcement agencies, and upon request, provide information related to the arrival of cargo/aircraft/passengers from foreign, to the extent permitted by law.

Business Partner Requirements

Air carriers must have written and verifiable processes for the screening of business partners, including carrier's agents and service providers. Air carriers must also have screening procedures for new customers, beyond financial soundness issues to include indicators of whether the customer appears to be a legitimate business and/or posse a security risk. Air carriers must also have procedures to review their customer's requests that could affect the safety of the aircraft or the cargo or otherwise raise significant security questions, including unusual customer demands.

Security procedures

Written or web-based procedures must exist for screening business partners which identify specific factors or practices, the presence of which would trigger additional scrutiny by the air carrier, up to and including a detailed physical inspection of the customer's cargo container/ULD prior to loading onto the aircraft. Particular attention should be given to house-to-house customer loaded containers/ULD.

For those business partners eligible for CTPAT certification (importers, consolidators, etc.) the air carrier must have documentation (e.g., CTPAT certificate, SVI number, etc.) indicating whether these business partners are or are not CTPAT certified. Non-CTPAT business partners should be subject to additional scrutiny by the air carrier.

Air carriers should ensure that contract aircraft service providers commit to CTPAT security recommendations through contractual agreements. Periodic reviews of the security commitments of the service providers should be conducted to detect weaknesses, or potential weaknesses, in security. Likewise, current or prospective business partners who have obtained a certification in a supply chain security program being administered by foreign Customs Administration should be required to indicate their status of participation to the air carrier.

Container or Unit Load Devices (ULD) Security

Air carriers must employ the use of high security seals (if and when applicable) and an accountable seal tracking process where cargo is transported via international cargo conveyance containers such as a ULD. In instances where cargo is not transported in a ULD, verifiable security methods must be put in to place to ensure, to the greatest extent possible, cargo is rendered tamper resistant and/or tamper evident. For all containers/ULDs in the air carrier's custody, container/ULD integrity must be maintained, to protect against the introduction of unauthorized material and/or persons. Air carriers must have documented procedures in place to maintain the integrity of the shipping containers/ULD and pallets in their custody. When an air carrier allows a ULD to leave their control, formal, verifiable procedures must be in place to track the ULD and its return into the carrier's custody.

Special considerations and security procedures must be developed for passenger flights carrying cargo. These processes must be documented and verifiable. Security procedures for passenger aircraft transporting cargo must include more intrusive examination of the cargo prior to packaging and loading, such as x-ray inspections, based on written articulated risk indicators. Security procedures during transport from the cargo area to the aircraft should be identified and known by all employees involved in the transportation.

Container/ULD Inspection

Air carriers must recognize the importance of a comprehensive inspection process prior to loading. The requirement to inspect all containers/ULDs, when used, prior to stuffing is placed upon the importers through the CTPAT Minimum Security Criteria for Importers dated March 25, 2005, yet air carriers must visually inspect all aircraft cargo hold areas, the exterior of any container/ULD, and the interior of the empty container/ULD, at the foreign port of lading. A seven-point inspection process is required for all empty containers/ULDs:

- Front wall
- Left side
- Right side
- Floor
- Ceiling/Roof
- Inside/outside doors
- Outside/Undercarriage

Container/ULD Seals

When containers/ULDs are used, written procedures must stipulate how seals in the air carrier's possession are to be controlled, and only designated employees must distribute seals for integrity purposes. Procedures should also exist for recognizing and reporting compromised seals and/or containers/ULDs to U.S. Customs and Border Protection or the appropriate foreign authority.

Container/ULD Storage

Containers/ULD must be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting and neutralizing unauthorized entry into container/ULD or container/ULD storage areas.

Physical Access Controls

Access controls prevent unauthorized entry to aircraft and facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, service providers and vendors at all points of entry. Contracted employees and service providers should only have access to those areas of the aircraft or facilities where they have legitimate business. Companies who contract for day workers or employ contract workers within warehouses or other areas not requiring airport or federal regulated badges, should include in their contract with the personnel providers that supplied workers for international cargo areas have undergone a security background check.

- **Boarding and Disembarking of Aircraft**

Consistent with the air carrier's security plan, all crew, employees, vendors and visitors are subject to a search when boarding or disembarking flights departing to or arriving from foreign. All crewmembers, employees, vendors, and visitors must display proper identification.

- **Employees**

An employee identification system must be in place for positive identification and access control purposes. Employees should only be given access to those secure areas needed for the performance of their duties. Company management or security personnel must adequately control the issuance and removal of employee, visitor and vendor identification badges. Procedures for the issuance, removal and changing of access devices (e.g. keys, key cards, etc.) must be documented.

- **Visitors / Vendors / Service Providers**

Visitors, vendors, and service providers must present photo identification for documentation purposes upon arrival, and a log must be maintained. All visitors and service providers should be escorted and visibly display temporary identification. Procedures must be in place to examine containers/ULDs added to the aircraft by service providers (i.e. food carts). CTPAT members
contracting vendors and service providers not eligible for participation in CTPAT must, by contract, require the providers to adhere to the minimum-security requirements for CTPAT.

- **Cargo Delivery Areas**

Delivery of goods to the consignee or other persons accepting delivery of cargo at the carrier's facility should be limited to a specific monitored area.

- **Challenging and Removing Unauthorized Persons**

Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.

Personnel Security

In compliance with applicable laws and regulations for that location, written and verifiable processes must be in place to screen prospective employees and to periodically check current employees.

- **Pre-Employment Verification**

Application information, such as employment history and references must be verified prior to employment.

- **Background checks / investigations**

Consistent with foreign, federal, state, and local regulations, background checks and investigations should be conducted for prospective employees. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.

- **Personnel Termination Procedures**

Companies must have procedures in place to immediately remove identification, facility, and system access for terminated employees.

Procedural Security

Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain. Procedures must be in place to prevent, detect, or deter unmanifested material and unauthorized personnel from gaining access to aircrafts, including concealment in cargo,

- **Passenger and Crew**

Air carriers must ensure compliance with the Advance Passenger Information System requirements so that accurate, timely and advanced transmission of data associated with international passengers and crew is provided to CBP. Procedures must be in place to record and report all anomalies regarding passenger and/or crew to U.S. Customs and Border Protection or other law enforcement agencies.

- **Bill of Lading / Manifesting Procedures**

Procedures must be in place to ensure that the information in the carrier's cargo manifest accurately reflects the information provided to the carrier by the shipper or its agent and is filed with CBP in a timely manner. Documentation control must include safeguarding computer access and information. Bill of lading information filed with CBP should show the first foreign port (place) where the air carrier takes possession of the cargo destined for the United States.

- **Cargo**

Cargo must be properly marked and manifested to include accurate weight and piece count. CBP and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected - as appropriate. Procedures to separate domestic cargo from international cargo in warehouses or pre-staging areas should be in place.

- **Aircraft**

Upon arrival of an international flight, the air carrier will provide CBP with assistance, upon request, to conduct intensive aircraft searches when deemed appropriate by CBP. Aircraft searches will be conducted by CBP Officers who will maintain the integrity of the aircraft and control entrance and egress until the aircraft search is compete.

Procedures must be in place to conduct physical inspections of the aircraft prior to loading of cargo or passenger. This will include:

- Inspection of all baggage hold areas
- Inspection of all overheads
- Inspection of all lavatories
- Inspection of all galleys and food carts
- Inspection of the cockpit and electronics areas
- Exterior inspection of all wheel wells and landing gears
- Inspection of avionic compartments/bays as warranted

Security Training and Threat Awareness

A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by terrorists at each point in the supply chain. Employees must be made aware of the procedures the air carrier has in place to address a situation and how to report it.

Additionally, specific training should be offered to assist employees in maintaining aircraft and cargo integrity, recognizing internal conspiracies, and protecting access controls. These programs should offer incentives for active employee participation.

Physical Security

Procedures must be in place to prevent, detect, or deter unmanifested material and unauthorized personnel from gaining access to the aircraft. Such measures are also covered by a facility's security plan. Cargo handling and storage facilities, container/ULD yards, and aircraft, in domestic and foreign locations, must have physical barriers and deterrents that guard against unauthorized access. Air carriers should incorporate the following CTPAT physical security criteria throughout their supply chains as applicable.

Fencing

Perimeter fencing should enclose the areas around cargo handling and storage facilities, container/ULD yards, and terminals. All fencing must be regularly inspected for integrity and damage.

Gates and Gate Houses

Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety.

Parking

Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas, and aircraft.

Building Structure

Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.

Locking Devices and Key Controls

All external and internal windows, gates and fences must be secured with locking devices. Management or security personnel must control the issuance of all locks and keys.

Lighting

Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas.

Alarms Systems & Video Surveillance Cameras

Alarm systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to aircraft, cargo handling and storage areas.

Cybersecurity

A system must be in place to identify the abuse of Information Technology (IT) including improper access, tampering, or the altering of business data. All system violators must be to appropriate disciplinary action.

- **Network Systems**

Network systems must be regularly tested for the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.

- **Sharing Information On Cybersecurity Threats**

IT policies should address how the company shares information on cybersecurity threats with the government and other business partners.

- **Identifying Abuse**

Systems 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.

- **Unauthorized Access**

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

- **Annual Review**

Cybersecurity policies and procedures must be reviewed annually.

- **User access**

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.

• **Individually Assigned Accounts**

Individuals with access to Information Technology (IT) systems must use individually assigned accounts. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication, and user access to IT systems must be safeguarded.

• **Passwords**

Passwords and/or passphrases must be regularly changed, but also changed as soon as possible if there is evidence of compromise or reasonable suspicion of a compromise exists. As well, passwords should be complex.

• **VPNs**

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.

• **Employee Devices**

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..

Trade-Based Money Laundering

Trade-Based Money Laundering occurs when criminals use the international trade system to disguise illicit proceeds by altering Customs and banking paperwork to make transactions appear legitimate. These proceeds are then used to finance additional criminal activity, which may include funding terrorist activities or organizations.

CTPAT Members and their business partners 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 criminal funding as there is a marked overlap between the two. Specialized training should be provided annually to personnel who may be able to identify the warning indicators of TradeBased Money Laundering and Terrorism Financing (examples of personnel who should receive this training include those responsible for trade compliance, security, procurement, finance, shipping, and receiving).

For further information, please consult the document CTPAT's Warning Indicators for TradeBased Money Laundering and Terrorism Financing Activities, as found on the Tricar Sales web site or the website of the U.S. Customs and Border Patrol CTPAT program.

The following are examples of some of the vetting elements that can help determine if a company is legitimate:

- Verifying the business address and how long they have been at that address.
- Conducting research on the internet on both the company and its principals.
- Checking business references.
- Requesting a credit report.

Upper Management Responsibility

The role of a company's upper management in CTPAT is to provide support and oversight to ensure the creation and maintenance of the company's Supply Chain Security Program. To this end, the designated company CTPAT administrator, head of security, or security coordinator should provide regular updates regarding the progress or outcomes of any audits, exercises, or validations to upper management.

To promote a culture of security, a letter of commitment to supply chain security (and/or the CTPAT program) should be signed by a senior company official and displayed in appropriate company locations.

Wood Packaging Materials, Pallets (Agricultural Procedures)

Visible pest contamination is to include compliance with Wood Packaging Materials (WPM) regulations. Measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15). This is a firm requirement of CTPAT as visible pest prevention measures must be adhered to throughout the supply chain.

Rail Carriers
CTPAT Security Procedures Guidelines

Rail carriers must conduct a comprehensive assessment of their security practices based upon the following CTPAT minimum-security criteria. Recognizing that rail carriers do not control their shippers and have a common carrier obligation to transport goods tendered to them, rail carriers shall work with their shippers on their security practices as set forth in these criteria.

These minimum-security criteria are fundamentally designed to be the building blocks for rail carriers to institute effective security practices designed to optimize supply chain performance to mitigate the risk of loss, theft, and contraband smuggling that could potentially introduce terrorists and implements of terrorism into the global supply chain.

Rail carriers should periodically assess their degree of vulnerability to risk and should prescribe security measures to strengthen or adjust their security posture to prevent security breaches and internal conspiracies. The determination and scope of criminal elements targeting world commerce through internal conspiracies requires companies.

C-T PAT recognizes the complexity of international supply chains and security practices and endorses the application and implementation of security measures based upon risk. Therefore, the program allows for flexibility and the customization of security plans based on the member's business model. Security measures, as listed throughout this document, must be implemented and maintained as appropriate to the carrier's business model and risk understanding.

Business Partner Requirements

Rail carriers must have written and verifiable processes for the screening of new business partners, including carrier's agents, sub-contracted rail carriers, and service providers, as well as screening procedures for new customers, beyond financial soundness issues to include security indicators. These processes apply to business partners and service providers not eligible for CTPAT membership.

Security Procedures

• Written procedures must exist to address specific factors or practices, the presence of which would trigger additional scrutiny by the rail carrier. U.S. Customs and Border Protection (CBP) will work in partnership with the rail carriers to identify specific information regarding what factors, practices or risks are relevant.

• For those business partners eligible for CTPAT certification (importers, ports, terminals, brokers, consolidators, carrier-forwarders, etc.) the Rail carrier must have documentation (e.g., CTPAT certificate) indicating whether these business partners are or are not CTPAT certified. Non-CTPAT business partners may be subject to additional scrutiny by the Rail carrier. Rail carriers should institute appropriate security procedures for their contract service providers.

• Rail carriers have a common carrier responsibility for all cargo loaded aboard their rail cars, they must communicate the importance of security to their employees as a fundamental aspect of their security policies.

• Rail carriers should strongly encourage that contract service providers and shippers commit to CTPAT security recommendations.

Rolling Stock Security

Rail carriers shall have procedures to protect against the introduction of unauthorized personnel and material.

• It is recognized that even though a carrier may not "exercise control" over the loading of rail cars and the contents of the cargo, rail carriers must be vigilant to guard against stowaways, and the smuggling of implements of terrorism and contraband. The rail carrier shall have procedures in place to guard against the loading of contraband while trains are in transit to the border, even in regard to unforeseen train stops.

• Rail carriers must have procedures in place for reporting unauthorized entry into rail cars, a and locomotives.

• Rail carriers must maintain inventory information and movement records on each rail car and use the physical rail car tracking technology that is inherent to the North American rail network system.

Inspection Procedures

• Rail personnel should be trained to inspect their rail cars and locomotives, for anomalies. Training in conveyance searches should be adopted as part of the company's on-the-job training program. Training that is held should be recorded or documented in a personnel file of the employee that attended the training.

• A systematic inspection must be made prior to reaching the U.S. border.

• During required on-ground safety inspections of rolling stock entering the U.S., conduct security inspections for any apparent signs of tampering, sabotage, attached explosives, contraband, stowaways, and other unusual or prohibited items. It is understood that railroads must comply with the Federal Railroad Safety Act and the Hazardous Materials Transportation Act.

• CBP will work in partnership with the rail carriers to identify specific information regarding what factors, practices or risks are relevant including the use of non-intrusive gamma ray technology or other inspections.

Conveyance Tracking and Monitoring Procedures

• Rail carriers must maintain, to the extent feasible and practicable, locomotive and rail car integrity while the train is en route to the U.S. border by maintaining inventory information and movement records for each rail car. Rail carriers must record unannounced or unforeseen train stops.

• Rail carriers must utilize existing tracking and monitoring processes to track conveyances while they are en route to the U.S. border. Unannounced or unforeseen train stops shall be documented.

• Railroad supervision must ensure that tracking and monitoring processes are being adhered to.

Seals

The sealing of rail cars, and intermodal maritime containers, along with continuous seal integrity are crucial elements of a secure supply chain and remains a critical aspect of a rail carrier's commitment to CTPAT. To the extent practical, a high security seal should be affixed to all loaded rail cars bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standards for high security seals. Rail carriers crossing the U.S. border must also fully comply with seal verification rules and seal anomaly reporting requirements once promulgated and mandated by the U.S. government.

• Clearly defined written procedures must stipulate how seals in the rail carrier's possession are to be controlled during transit. These written procedures should be briefed to all rail crewmembers and there should be a mechanism to ensure that these procedures are understood and are being followed. These procedures must include:

Physical Access Controls

To the extent practical, rail carriers should institute access controls to prevent unauthorized entry to rail property and rail cars and should maintain control of employees and visitors. Access controls should include the positive identification of employees, visitors, service providers, and vendors. Rail companies should also conduct spot inspections of motor vehicles on railroad property where international shipments are handled.

- **Employees**

An employee identification system must be in place for positive identification and access control purposes. Employees should only be given access to high security areas such as dispatch centers if necessary for the performance of their duties. Railroad supervision or railroad police must adequately control the issuance and removal of employee, visitor and vendor identification badges. Procedures for the issuance, removal and changing of access devices (e.g. keys, key cards, etc.) must be documented. Establish employee identification measures for all employees. Conduct spot checks of identification as threat conditions warrant.

- **Visitors, Vendors and Service Providers**

To the extent feasible and practicable, and as threat conditions warrant, restrict the access of contractors and visitors to non-public areas of company-designated critical infrastructure and monitor the activities of visitors in or around such infrastructure.

- **Challenging and Removing Unauthorized Persons**

Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.

- **Unauthorized Persons**

  − Implement measures to deter unauthorized entry and increase the probability of detection at company-designated critical infrastructure. Provide safety and security training for employees at facilities where international shipments are handled.

  − Establish procedures to detect or deter unmanifested material and unauthorized personnel from gaining access to trains crossing into the United States.

  − Reinforce the need for employees to immediately report to the proper authorities all suspicious persons, activities, or objects encountered.

  − Focus proactive community safety and security outreach and trespasser abatement programs in areas adjacent to company-designated critical infrastructure to reduce the likelihood of unauthorized individuals on company property and to enhance public awareness of the importance for reporting suspicious activity.

Personnel Security

Written and verifiable processes must be in place to screen prospective rail employees and to periodically check current employees.

• **Pre-Employment Verification / Background Checks / Investigations**
Application information, such as employment history and references must be verified prior to employment.
• **Background checks/investigations**
Depending on the sensitivity of the position, background checks and investigations shall be conducted for current and prospective employees as appropriate and as required by foreign, federal, state and local.,,. regulations. Conduct background checks on all new railroad employees. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.
• **Personnel Termination Procedures**
Companies must have procedures in place to remove identification, facility, and system access for terminated employees.

Procedural Security

Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain. Procedures must be in place to prevent, detect, or deter unmanifested material and unauthorized personnel from gaining access to rail cars and locomotives.

Security procedures should be implemented that restricts access to the rail car and locomotive and prevents the lading of contraband while en-route from facilities in international locations to the United States.

Procedures must be in place to record and immediately report all anomalies regarding train crew personnel to U.S. Customs and Border Protection. Likewise, rail companies should investigate all suspicious activity and report it to the proper authority.

Bill of Lading/Manifesting Procedures
Procedures must be in place to ensure that the information in the carrier's cargo manifest accurately reflects the information provided to the carrier by the shipper or its agent and is filed with CBP in a timely manner. Documentation control must include safeguarding computer access and information.

• **Reporting Train Crew Personnel**
Identify all personnel on the train as required by CBP.

• **Reporting Suspicious Cargo**
All instances of suspicious cargo shipments should be reported immediately to the nearest CBP port-of-entry or other nearest appropriate authority.

Physical Security

Procedures must be in place to prevent, detect, or deter unmanifested material and unauthorized personnel from gaining access to conveyance, including concealment in rail cars. Rail carriers should incorporate the following CTPAT physical security criteria throughout their supply chains as applicable.

- **Fencing**

Perimeter fencing should enclose areas deemed by the rail carrier to be a critical infrastructure.

- **Parking**

Privately owned vehicles should be monitored when parked in close proximity to rolling stock that crosses the international border.

- **Building Structure**

Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.

- **Lighting**

Adequate lighting must be provided where appropriate, for entrances and exits.

- **Alarms Systems & Video Surveillance**

Cameras Where appropriate, alarm systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to rail property.

Security Training and Threat Awareness

A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by drug smugglers and terrorists. Employees must be made aware of the procedures the rail carrier has in place to address a situation and how to report it.

Additionally, specific training should be offered to assist employees in maintaining rolling stock integrity, recognizing internal conspiracies, and protecting access controls

- Establish an employee security awareness-training program to include procedures to recognize suspicious activity and report security concerns.
- During required on-ground safety inspections of international shipments inspect for any apparent signs of tampering, sabotage, attached explosives, and other suspicious items. Train employees to recognize suspicious activity and report security concerns found during inspections and in transit.
- Implement a policy to preclude unnecessary disclosure of sensitive information.

Cybersecurity

A system must be in place to identify the abuse of IT, including improper access, tampering, or the altering of business data. All system violators must be to appropriate disciplinary action.

- **Network Systems**

Network systems must be regularly tested for the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.

- Sharing Information On Cybersecurity Threats

A carrier's IT policies should address how the carrier shares information on cybersecurity threats with the government and other business partners.

- **Identifying Abuse**

Systems 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.

- **Unauthorized Access**

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

- **Annual Review**

Cybersecurity policies and procedures must be reviewed annually.

- **User access**

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.

- **Individually Assigned Accounts**

Individuals with access to Information Technology (IT) systems must use individually assigned accounts. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication, and user access to IT systems must be safeguarded.

- **Passwords**

Passwords and/or passphrases must be regularly changed, but also changed as soon as possible if there is evidence of compromise or reasonable suspicion of a compromise exists. As well, passwords should be complex.

- **VPNs**

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.

- **Employee Devices**

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..

Trade-Based Money Laundering

Trade-Based Money Laundering occurs when criminals use the international trade system to disguise illicit proceeds by altering Customs and banking paperwork to make transactions appear legitimate. These proceeds are then used to finance additional criminal activity, which may include funding terrorist activities or organizations.

CTPAT Members and their business partners 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 criminal funding as there is a marked overlap between the two. Specialized training should be provided annually to personnel who may be able to identify the warning indicators of Trade-Based Money Laundering and

Terrorism Financing (examples of personnel who should receive this training include those responsible for trade compliance, security, procurement, finance, shipping, and receiving).

For further information, please consult the document CTPAT's Warning Indicators for Trade-Based Money Laundering and Terrorism Financing Activities on the Tricar Sales Inc. website or the website of the U.S. Customs and Border Patrol CTPAT program.

The following are examples of some of the vetting elements that can help determine if a company is legitimate:

- Verifying the company's business address and how long they have been at that address.
- Conducting research on the internet on both the company and its principals.
- Checking business references.
- Requesting a credit report.

Upper Management Responsibility

The role of a company's upper management in CTPAT is to provide support and oversight to ensure the creation and maintenance of the company's Supply Chain Security Program. To this end, the designated company CTPAT administrator, head of security, or security coordinator should provide regular updates regarding the progress or outcomes of any audits, exercises, or validations to upper management.

To promote a culture of security, a letter of commitment to supply chain security (and/or the CTPAT program) should be signed by a senior company official and displayed in appropriate company locations.

Wood Packaging Materials, Pallets (Agricultural Procedures)

Visible pest contamination is to include compliance with Wood Packaging Materials (WPM) regulations. Measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15). This is a firm requirement of CTPAT as visible pest prevention measures must be adhered to throughout the supply chain.

-- continued below --

Ocean Transportation Intermediaries and NVOCCs

(Non-Vessel Operating Common Carriers)

CTPAT Security Procedures Guidelines

Consolidators must conduct a comprehensive assessment of their international supply chains based upon the following CTPAT security Procedures guidelines. Where a consolidator outsources or contracts elements of their supply chain, such as a foreign facility, conveyance, domestic warehouse, or other elements, the consolidator must work with these business partners to ensure that pertinent security measures are in place and adhered to throughout their supply chain. The supply chain for CTPAT purposes is defined from point of origin (manufacturer/supplier/vendor) through to point of distribution and recognizes the diverse business models CTPAT members employ. CTPAT recognizes the complexity of international supply chains and endorses the application and implementation of security measures based upon risk analysis. Therefore, the program allows for flexibility and the customization of security plans based on the member's business model. Appropriate security measures, as listed throughout this document, must be implemented and maintained throughout the consolidator's supply chains.

Business Partner Requirements

Consolidators must have written and verifiable processes for the screening and selection of business partners, including foreign consolidators, customers, contractors, carriers, and vendors. Ensure that contracted service provider companies who provide transportation, cargo handling, and security services commit to CTPAT security procedures guidelines. Periodically review the performance of the service providers to detect weakness, or potential weakness, in security.

Security Procedures

- **Point of Origin**

C-TPAT Consolidators must ensure that business partners develop security processes and procedures consistent with the CTPAT security procedures guidelines to enhance the integrity of the shipment at point of origin. Periodic reviews of business partners' processes and facilities should be conducted based on risk, and should maintain the security standards required by the Consolidator.

- **Participation/Certification in Foreign Customs Administrations Supply Chain Security Programs**

Current or prospective business partners who have obtained a certification in a supply chain security program administered by foreign Customs Administration should be required to indicate their status of participation to the CTPAT Consolidator.

- **Service Provider Screening and Selection Procedures**

The CTPAT Consolidator should have documented service provider screening and selection procedures to screen the contracted service provider for validity, financial soundness, ability to meet contractual security requirements, and the ability to identify and correct security deficiencies as needed. Service Provider procedures should use a risk-based process as determined by an internal management team.

- **Customer Screening Procedures**

The CTPAT Consolidator should have documented procedures to screen prospective customers for validity, financial soundness, the ability to meet contractual security requirements, and the ability to identify and correct security deficiencies as needed. Customer screening procedures should use a risk-based process as determined by an internal management team.

Container Security

Consolidators should ensure that all contracted service providers have procedures in place to maintain container integrity. Container integrity must be maintained to protect against the introduction of unauthorized material and/or persons. At point of stuffing, procedures must be in place to properly seal and maintain the integrity of the shipping containers. A high security seal must be affixed to all loaded CTPAT importer containers bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standards for high security seals.

- **Container Inspection**

Procedures must be in place to verify the physical integrity of the container structure prior to stuffing, to include the reliability of the locking mechanisms of the doors. A 7-point inspection process is recommended for all containers: 1. Front wall 2. Left side 3. Right side 4. Ceiling/Roof 5. Inside/Outside doors 6. Outside/Undercarriage 7. Floor

- **Container Seals**

Written procedures must stipulate how seals are to be controlled and affixed to loaded containers. Procedures must be in place for recognizing and reporting compromised seals and/or containers to U.S. Customs and Border Protection, or the appropriate foreign authority. Only designated employees should distribute container seals for integrity purposes.

- **Container Storage**

Containers must be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting and neutralizing unauthorized entry into containers or container storage areas.

Physical Access Controls

Access controls prevent unauthorized entry to facilities, maintain control of employees and visitors and protect company assets. Access controls must include the positive identification of all employees, visitors, and vendors at all points of entry.

- **Employees**

An employee identification system must be in place for positive identification and access control purposes. Employees should be given access only to those secure areas needed for the performance of their duties. Company management or security personnel must adequately control the issuance and removal of employee, visitor, and vendor identification badges. Procedures for the issuance, removal, and changing of access devices (e.g. keys, key cards, etc.) must be documented.

- **Visitors Controls**

Visitors must present photo identification for documentation purposes upon arrival. All visitors should be escorted and visibly display temporary identification.

- **Deliveries (including mail)**

Proper vendor ID and/or photo identification must be presented for documentation purposes by all vendors. Arriving packages and mail should be periodically screened before being disseminated.

- **Challenging and Removing Unauthorized Persons**

Procedures must be in place to identify, challenge, and address unauthorized/unidentified persons.

Personnel Security

Processes must be in place to screen prospective employees and to periodically check current employees. Maintain a current permanent employee list (foreign and domestic), which includes the name, date of birth, national identification number or social security number, and position held, and submit such information to CBP upon written request, to the extent permitted by law.

- **Pre-Employment Verification**

Application information, such as employment history and references must be verified prior to employment.

- **Background checks / investigations**

Consistent with foreign, federal, state, and local regulations, background checks, and investigations should be conducted for prospective employees. Periodic checks and reinvestigations should be performed based on cause and/or the sensitivity of the employee's position.

- **Personnel Termination Procedures**

Companies must have procedures in place to remove identification, as well as facility and system access for terminated employees.

Procedural Security

Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain.

- **Documentation Processing**

Procedures must be in place to ensure that all documentation used in the movement of merchandise/cargo is legible, complete, accurate, and protected against the exchange, loss, or introduction of erroneous information. Documentation control must include safeguarding computer access and information.

- **Manifesting Procedures**

To help ensure the integrity of cargo received from abroad, procedures must be in place to ensure that information received from business partners is reported accurately and in a timely manner.

- **Shipping & Receiving**

Arriving cargo should be reconciled against information on the cargo manifest. The cargo should be accurately described, weighed, labeled, marked, counted, and verified. Departing cargo should be checked against purchase or delivery orders. Drivers delivering or receiving cargo must be positively identified before cargo is received or released.

- **Cargo Discrepancies**

All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. CBP and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected.

Security Training and Threat Awareness

A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by terrorists at each point in the supply chain. Employees must be made aware of the procedures the company has in place to address a situation and how to report it. Additional training should be provided to employees in the shipping and receiving areas, as well as those receiving and opening mail.

Additionally, specific training should be offered to assist employees in maintaining cargo integrity, recognizing internal conspiracies, and protecting access controls. These programs should offer incentives for active employee participation.

Physical Security

Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access. Consolidators should incorporate the following CTPAT physical security guidelines throughout their supply chains as applicable:

- **Fencing**

Perimeter fencing should enclose the areas around cargo handling and storage facilities. Interior fencing within a cargo handling structure should be used to segregate domestic, international, high value, and hazardous cargo. All fencing must be regularly inspected for integrity and damage.

- **Gates Gate Houses**

Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety.

- **Parking**

Private passenger vehicles should be prohibited from parking in, or adjacent to, cargo handling and storage areas.

- **Building Structure**

Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.

- **Locking Devices and Key Controls**

All external and internal windows, gates, and fences must be secured with locking devices. Management or security personnel must control the issuance of all locks and keys.

- **Lighting**

Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, cargo handling, storage areas, fence lines, and parking areas.

- **Alarms Systems & Video Surveillance Cameras**

Alarm systems and video surveillance cameras should be used to monitor premises and prevent unauthorized access to cargo handling and storage areas.

Cybersecurity

A system must be in place to identify the abuse of IT, including improper access, tampering, or the altering of business data. All system violators must be to appropriate disciplinary action.

- **Network Systems**

Network systems must be regularly tested for the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.

- **Sharing Information On Cybersecurity Threats**

Company IT policies should address how the company shares information on cybersecurity threats with the government and other business partners.

- **Identifying Abuse**

Systems 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.

- **Unauthorized Access**

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

- **Annual Review**

Cybersecurity policies and procedures must be reviewed annually.

- **User access**

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.

- **Individually Assigned Accounts**

Individuals with access to Information Technology (IT) systems must use individually assigned accounts. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication, and user access to IT systems must be safeguarded.

- **Passwords**

Passwords and/or passphrases must be regularly changed, but also changed as soon as possible if there is evidence of compromise or reasonable suspicion of a compromise exists. As well, passwords should be complex.

- **VPNs**

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.

• **Employee Devices**
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..

Trade-Based Money Laundering

Trade-Based Money Laundering occurs when criminals use the international trade system to disguise illicit proceeds by altering Customs and banking paperwork to make transactions appear legitimate. These proceeds are then used to finance additional criminal activity, which may include funding terrorist activities or organizations.

CTPAT Members and their business partners 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 criminal funding as there is a marked overlap between the two. Specialized training should be provided annually to personnel who may be able to identify the warning indicators of TradeBased Money Laundering and Terrorism Financing (examples of personnel who should receive this training include those responsible for trade compliance, security, procurement, finance, shipping, and receiving).

For further information, please consult the document CTPAT's Warning Indicators for TradeBased Money Laundering and Terrorism Financing Activities on the Tricar Sales Inc website or the website of the U.S. Customs and Border Patrol CTPAT program.

The following are examples of some of the vetting elements that can help determine if a company is legitimate:

- Verifying the company's business address and how long they have been at that address.
- Conducting research on the internet on both the company and its principals.
- Checking business references.
- Requesting a credit report.

Upper Management Responsibility

The role of a company's upper management in CTPAT is to provide support and oversight to ensure the creation and maintenance of the company's Supply Chain Security Program. To this end, the designated company CTPAT administrator, head of security, or security coordinator should provide regular updates regarding the progress or outcomes of any audits, exercises, or validations to upper management.

To promote a culture of security, a letter of commitment to supply chain security (and/or the CTPAT program) should be signed by a senior company official and displayed in appropriate company locations.

Wood Packaging Materials, Pallets (Agricultural Procedures)

Visible pest contamination is to include compliance with Wood Packaging Materials (WPM) regulations. Measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15). This is a firm requirement of CTPAT as visible pest prevention measures must be adhered to throughout the supply chain.

[end document]

For more information: Please contact Tricar Sales at email address: info@tricarsales.com

CERTIFICATION COORDINATOR