A Message Regarding Security-Procedures Guidelines for Customs Brokers

Tricar Sales Inc. is a participant in the Customs-Trade Partnership Against Terrorism (CTPAT).

CTPAT is a voluntary joint government-business initiative to build cooperative relationships that strengthen the overall supply chain, and border security. Every person who is involved in logistics, distribution, or supply chain management will be affected by ongoing efforts to create a more secure global trading system. Importers are now expected to be able to demonstrate that all aspects of this process are under control throughout the supply chain.

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 follow security processes and procedures consistent with CTPAT security criteria. Hence, we request that you provide one of the following documents to verify compliance with CTPAT guidelines.

- Copy of CTPAT Certification (Preferred)
- Certification of participation in a foreign Customs security program (overseas brokers)
- Documentation from a corporate officer attesting to compliance.
- Completion of a security-procedures questionnaire.

Please provide this information to us as soon as you receive our communications to you requesting it. If you should have any questions, please contact us by replying to the email by which you received this message.

For your convenience we have provided further information below (Customs Brokers Security Procedures Guidelines) regarding the CTPAT program and security concerns. However, brokers are reminded that it is very important to seek out and be familiar with the CBP's most recent Minimum-Security Criteria for their industry sector.

Best regards,
Tricar Sales

Customs Brokers

CTPAT Security-Procedures Guidelines

U.S. Customs brokers must conduct a comprehensive assessment of their security practices based upon the following CTPAT minimum-security criteria. Brokers play a decisive role in the transmission of key trade data and as a liaison between U.S. Customs and Border Protection (CBP) and other key entities in the supply chain. In this capacity, the broker's key role – besides the transmission of data - is to educate, corroborate, and encourage others within supply chain further the tenets of supply chain security.

The below minimum-security criteria are designed to help your company institute or verify effective security practices designed to optimize supply chain performance so as to mitigate the possibility that terrorists and criminals could exploit a supply chain. Strong security measures reduce loss, theft, contraband smuggling and the introduction of terrorism and other crime into the global supply chain. The supply chain for CTPAT purposes is defined from point of origin (manufacturer/supplier/vendor) through to point of distribution (customer).

CTPAT recognizes the complexity and diversity of international supply chains and business models 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. However, appropriate security measures, as listed throughout this document, must be implemented and maintained throughout the Broker's business model, based on risk.

Cybersecurity

Brokers 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, and must follow cybersecurity protocols that are based on recognized industry frameworks/standards. For example:

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 broker’s IT policies should address how the broker 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).

It is strongly recommended that you seek out and consult the document CBP's Warning Indicators for Trade-Based Money Laundering and Terrorism Financing Activities, as found on the CBP's CTPAT website page for your industrial sector.

The following are just a few examples of vetting elements that can help determine if a potential business-partner 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.

There are many, many ways your company could be victimized or inadvertently help victimize a client company. Again, we strongly recommended that you seek out and consult the document CBP's Warning Indicators for Trade-Based Money Laundering and Terrorism Financing Activities.

Business Partner Requirement

Unless otherwise expressly indicated, for purposes of implementing the minimum standards prescribed in this section, the term "business partner" will include all third parties within the supply chain with whom the Customs broker voluntarily, and on its own initiative, engages in the performance of its agency obligations for importer clients (but does not include those clients).

Brokers must have written and verifiable processes for the screening of new business partners, beyond financial soundness issues, to include security indicators.

Written procedures must exist to address the specific factors or practices as (determined by CBP) as sufficient to trigger additional scrutiny of the import transaction. CBP will work in partnership with the brokers to identify specific information regarding what factors, practices or risks are relevant.

For business partners eligible for CTPAT certification, the Customs broker must have documentation (e.g., CTPAT certification letter, etc.) indicating whether these business partners are, or are not CTPAT certified. Current or prospective business partners who have obtained a certification in a supply chain security program being administered by foreign (non-U.S.) Customs Administration should be required to indicate their status of participation to the broker. To the extent such information can be obtained, brokers will maintain secure provider lists of CTPAT certified (or equivalent) service providers in all relevant categories.

For client-importers, brokers must ensure that CTPAT security criteria is provided by making educational opportunities available through seminars, through consultative services, dissemination of text materials, and/or through aiding clients in obtaining such materials on the CBP website or elsewhere, when requested. The brokers must develop and document a process for handling security related client-importer inquiries. Brokers should encourage client-importers to join the CTPAT program.

Container & Trailer Security

Customs brokers must convey to their business partner importers, whether a CTPAT member or not, the criticality of having security procedures in place at the point of stuffing, and procedures to inspect, properly seal and maintain the integrity of the shipping containers and trailers. Customs brokers should also convey to their business partners, that the seven-point inspection process for empty containers prior to the loading the cargo, as well as the seventeen-point inspection process for all trailers/tractors, should be followed. Supporting documentation can be found on the CBP's CTPAT website.

Container & Trailer Seals

The sealing of trailers and containers – and their continuous seal integrity as they travel -- are crucial elements of a secure supply chain. brokers should convey to their business partners that seals used to secure loaded containers and trailers bound for the U.S. must meet or exceed the current PAS ISO 17712 standards for high security seals.

Remind all client-importers that all loaded U.S.-bound containers and trailers must have a PAS ISO 17712 high-security seal affixed.

When necessary, the broker should also inform their business partners that they must institute procedures for recognizing and reporting compromised seals to CBP or the appropriate foreign authority.

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.

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 and visitors at all points of entry.

Employees

For all brokers, procedures for the issuance, removal and changing of access devices (e.g. keys, key cards, etc.) must be documented. In addition, for broker facilities at which there is in excess of 50 employees, a security identification system must be in place for positive identification and access control purposes, under which company management or security personnel will maintain and adequately control the issuance and return of employee photo identification badges or equivalent control.

Visitors

For documentation purposes, unknown visiting persons should be required to present photo identification upon arrival and should be escorted while on the broker's premises. The broker should maintain a logbook or electronic diary of all unknown visiting persons, recording such data as visitor name, purpose of visit and confirmation of identity. In addition, for the broker category of facilities in excess of 50 employees, all visitors/vendors should be provided temporary identification badges upon arrival, to be visibly displayed at all times while on the brokers premises.

Challenging and Removing Unauthorized Persons

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

Deliveries (including mail)

Proper vendor ID and/or photo identification must be presented for documentation purposes

upon arrival of all first time/unknown vendors or vendor representatives. At times of heightened alert involving package and mail delivery, these items should be screened before being disseminated.

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

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

Customs brokers 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 of any data or documents relevant to the security of processes, transportation, handling, and storage of cargo in the supply chain.

Customs brokers should notify CBP, and/or other law enforcement agencies as specified by CBP for these purposes, whenever anomalies or illegal activities related to security issues are detected or suspected.

Documentation Processing

Measures should be in place to ensure that data transmitted by the Customs broker is of optimal quality in order for CBP to maximize the use of automated targeting and other screening tools for cargo release or designation for a physical examination. Procedures must be in place to ensure that all information provided by the importer/exporter, freight forwarder, etc., and used in the clearing of merchandise/cargo, is legible and protected against the exchange, loss or introduction of erroneous information.

Documentation controls for the broker should include procedures for:

− Ensuring the consistency of information transmitted to CBP through the entry summary process with the information that appears on the transaction documents provided to the broker, with regard to such data as the supplier and consignee name and address, commodity description, weight, quantity, and unit of measure (i.e. boxes, cartons, etc.) of the cargo being cleared.

− Review of documentation for completeness and clarity and contacting the business partner or importer/exporter, as necessary, to obtain corrected documentation or information,

− To the extent such information comes to the broker's attention, alerting the importer/exporter of its obligation to notify CBP and/or any other appropriate law enforcement agency of any errors and/or shortages and overages of merchandise that create a security risk in the supply chain, and providing assistance that is consistent with its for hire services in making such notification and correction of data as may be required or requested by the importer/exporter.

Advanced Submission of Data

CTPAT importers who are currently NOT filing entry prior to the arrival of their cargo in the port of arrival are not receiving their full CTPAT benefits, especially reduced examinations.

To fully realize the reduced cargo examinations afforded to certified and validated CTPAT importers, entry must be made to CBP as early in the importation process as possible, and at a minimum, of 24 hours prior to the cargo arriving to the first port of entry within the United States. The reason this is necessary is that CTPAT benefits are aligned with a CTPAT members' importer of record number. The importer of record number only becomes known when entry is filed; importer of record numbers are

not identified on manifest information. To receive full benefits, the entry should be filed prior to arrival of the cargo.

This applies only to cargo imported via ocean transport (sea containers), and not to cargo arriving via other modes of transport

Cargo Discrepancies

All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or CBP and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities anomalies are detected or suspected- as appropriate. The broker will ensure that the client-importer is aware of the following:

The discrepancy or anomaly must be fully investigated. Customs and/or other appropriate law enforcement agencies, as appropriate, should be notified of such discrepancy or anomaly.

Consistent with its for hire services, the broker can assist in the reporting of the anomaly and will make appropriate modifications in the transmission of entry data.

Shipping & Receiving

Arriving cargo should be reconciled against information on the cargo manifest. The cargo should be accurately described, and the weights, labels, marks and piece count indicated and verified. Cargo should be verified against purchase or delivery orders. Drivers delivering or receiving cargo must be positively identified before the cargo is received or released. Procedures should also be established to track the timely movement of incoming goods.

Physical Security

Cargo handling and storage facilities, as well as those facilities used to make entry of international cargo, must have physical barriers and deterrents that guard against unauthorized access. Brokers should incorporate the following CTPAT physical security criteria throughout their supply chains as applicable. (Note: CTPAT is cognizant of the diverse business models that Brokers employ and takes into consideration that the physical security measures outlined in this document may not correspond

to the business model of some CTPAT brokers.) Of course, they are to be sought out in business partners.

Fencing

Perimeter fencing should enclose the areas around cargo handling and storage facilities. When required by CBP, 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 and Gate Houses

Security 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

Where substantially comparable alternative parking is available, 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.

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

When reasonably and specifically required by CBP, alarm systems and video surveillance cameras must be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas.

Physical Security

Cargo handling and storage facilities, as well as those facilities used to make entry of the international cargo, must have physical barriers and deterrents that guard against unauthorized access.

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. Office buildings must have after hour access limited.

Security Training and Threat Awareness

As a liaison between CBP and trade community, the broker should create opportunities to educate the importing community on CTPAT policy, and those areas in which the broker has relevant expertise, which might include security procedures, best practices, access controls, documentation fraud, information security, internal conspiracies, and technologies that further the goal of a secure global supply chain. These interactions should focus on employees working in shipping, information technology, receiving and mailroom processing.

A security awareness program should also include notification being provided to CBP and other law enforcement agencies whenever anomalies or illegal activities related to security are detected or suspected.

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.

[end document]

[end document]

CERTIFICATION COORDINATOR