EXPECTATION OF SECURITY FOR FREIGHT AND LANE SEGMENTS
Prepared by Griffin & Company Logistics

The Customs-Trade Partnership Against Terrorism (C-TPAT) workgroup at William L. Griffin & Company, Inc. D/B/A Griffin & Company Logistics (Griffin) respectfully requests that this document be forwarded to, and read by the operations manager, or highest officer involved with the manufacture, stuffing, consolidation, shipping, or movement for importation, or exportation of freight at any level.

The security of freight, and the lane segments by which it travels is of the utmost importance. Not only does it involve the security of your country, but can also impact your business, and your employees.

The materials in this document are directly derived from U.S. Customs & Border Protections C-TPAT Minimum Security Criteria. Griffin fully supports these requirements, and suggestions. Griffin also expects, it's business partners to follow these practices to the best of their abilities. Understandably, not every practice herein applies to every business partner. It is important however to be aware of these practices as they may apply to other businesses in contact in the supply chain.

Adhering to these practices is a continuing path of growth within any organization. Increased diligence in security will benefit each business, and the supply chain as a whole.

If this is new to a business, the task of designing a program may seem insurmountable. But each step selected, worked upon, and completed improves a business's supply chain security program.

Griffin has the following representatives involved in the workgroup with the C-TPAT program:

Robert A. Hanson, Vice President of Operations (primary contact for C-TPAT)
William L. Griffin, Chairman
Erin G. Doyle, President
Tyler Peterson, Vice President of Warehouse Operations
Michael W. Holetz, Sales, and Marketing
Michael A. Finnegan, Senior Administrator
Toua C. Yang, Operations Supervisor, Transportation Security Administration (TSA) Primary Contact

Expectation of Security

Security Management

Each business partner's supply chain security program should be designed with, supported by, and implemented by an appropriate written review component, or policy to document that a system is in place whereby personnel are held accountable for their responsibilities, and all security procedures outlined by the security program are being carried out as designed

The review plan, or policy should be updated as needed based on pertinent changes in the organization's operations, and level of risk. A supply chain security audit program that includes how often is it updated should be implemented.

Upper management should provide support, and oversight to ensure the creation and maintenance of the company's Supply Chain Security Program. An easily identifiable point(s) of contact (POC) should be assigned to provide regular updates regarding the progress or outcomes of any audits, exercises, or validations in the security program.
Points of contact need to be trained and knowledgeable about the business's security program requirements, and their responsibilities within that program.

Upper management should provide a documented statement of support.

Risk Assessment

The amount of risk in the supply chain needs to be documented. An overall risk assessment to identify threats, assess risks, and incorporate sustainable measures to mitigate vulnerabilities should be conducted to identify where security vulnerabilities may exist. These risk assessments should be reviewed annually at a minimum, or more frequently as risk factors dictate.

Written procedures should be in place that address crisis management, business continuity, security recovery plans, and business resumption.

Business Partners

A written, risk-based process is needed for screening new business partners, and for monitoring current partners. Screening should include checks on activity related to money laundering, and terrorist funding based on risk, and key warning indicators as they are most applicable to the functions performed by the business in the supply chain.

Business partner screening should also include background, or reference checks including membership of relevant trade organization (including any membership of mutually recognized agreement organizations such as AEO, C-TPAT, etc.). Evidence of this membership should be obtained on a periodic basis.

Documents of importation, and exportation should be reviewed to identify, or recognize suspicious cargo shipments? (originated from or destined to unusual locations, paid by cash, or a certified check, using unusual routing methods, exhibit unusual shipping/receiving practices; and provide vague, generalized, or a lack of any pertinent information).

Due diligence needs to be exercised in outsourcing, or contracting elements of the supply chain to ensure these business partners have security measures in place that meet, or exceed minimum security criteria.
To ensure that business partners continue to comply with minimum security criteria, security assessments of business partners should be reviewed, and updated on a regular basis, or as circumstances/risks dictate.

Client importers, and other business partners must be apprised of security requirements, and critical program developments as they relate to C-TPAT, and other supply chain security programs. Client importers are encouraged to become CTPAT Members.

Procedural Security

Procedures must be in place to ensure that all information used in the clearing of merchandise/cargo is legible, complete, accurate, protected against the exchange, loss, or introduction of erroneous information, and reported on time (timely, accurate and protected). Accuracy should include weight, and piece counts.

Arriving cargo should be reconciled against information on the cargo manifest. Departing cargo should be verified against purchase or delivery orders.

The shipper, or its agent must ensure that bill of ladings (BOLs), and/or manifests accurately reflect the information provided to the carrier, and carriers must exercise due diligence to ensure these documents are accurate. BOLs, and manifests must be filed with proper authorities, and (US) Customs & Border Protection (CBP) in a timely manner. The BOL information filed with CBP must show the first foreign location/facility where the carrier takes possession of the cargo destined for the United States.

If paper is used, forms, and other import/export related documentation should be secured to prevent unauthorized use.

When cargo is staged overnight, or for an extended period of time, measures must be taken to secure the cargo from unauthorized access. Loading, and stuffing of cargo into containers/IIT should be supervised by a security officer, or manager, or other designated personnel. Arriving cargo should be reconciled against information on the cargo manifest. Departing cargo should verified against purchase or delivery orders.

All shortages, overages, and other significant discrepancies, or anomalies must be investigated, and those investigations must be resolved, as appropriate.

Procedures must be in place to identify, challenge, and address unauthorized, and unidentified persons. Company personnel must be trained to know the protocol to challenge an unknown, unauthorized person, how to respond to the situation, and be familiar with the procedure for causing the removal of an unauthorized individual from the premises.

Written procedures must be in place for reporting a security related incident to include a description of the facility's internal escalation process for reporting. A notification protocol must also be in place to report any suspicious activities, or security incidents that may affect the security of the business partner's supply chain. As applicable, incidents must be reported to the proper authorities, the closest port of entry, any pertinent law enforcement agencies, and business partners that may be part of the affected supply chain.

Procedures must include accurate contact information that lists the name(s), and phone number(s) of personnel requiring notification, as well as for law enforcement agencies. Notifications to relevant government agencies should be made as soon as feasibly possible, and in advance of any conveyance, or IIT crossing a border. These Procedures must be periodically reviewed to ensure contact information is accurate.

Consistent with for hire services, clients must be advised of their obligation to report any anomalies to the proper authorities or CBP (US), and/or any other appropriate law enforcement agencies. If applicable, clients must be advised to make all required modifications so that the correct data is transmitted.

The business should establish a way to report security related issues anonymously. When an allegation is received, it should be investigated, and if applicable, corrective actions taken.

Internal investigations must be performed immediately after an incident. The investigation must be documented.

Conveyance & IIT

Conveyances and Instruments of International Traffic (IIT) must be stored in a secure area to prevent unauthorized access, which could result in an alteration to the structure of an Instruments of International Traffic, or (as applicable) allow the seal/doors to be compromised.

Written procedures must be in place for both security and agricultural inspections of IIT.

Prior to loading, stuffing, or packing, all conveyances, and empty IIT must undergo security and agricultural inspections to ensure their structures have not been modified to conceal contraband, or have not been contaminated with visible agricultural pests. A seven-point inspection on all empty containers and unit load devices (ULD) includes inspection on:

- Front wall.
- Left side.
- Right side.
- Floor.
- Ceiling/Roof.
- Inside/outside doors (including the reliability of the locking mechanisms of the doors).
- Outside/Undercarriage.

An eight-point inspection on all empty refrigerated containers and ULDs conducted prior to loading/stuffing to includes inspection on:

- Front wall.
- Left side.
- Right side.
- Floor.
- Ceiling/Roof.
- Inside/outside doors (including the reliability of the locking mechanisms of the doors).
- Outside/Undercarriage.
- Fan housing on refrigerated containers.

The seventeen-point inspection on all tractor/trailer units conducted prior to the movement of containers includes inspection on:

- Bumper/tires/rims (tractors).
- Doors, tool compartments, and locking mechanisms (tractors).
- Battery box (tractors).
- Air breather (tractors).
- Fuel tanks (tractors).
- Interior cab compartments/sleeper (tractors).
- Faring/roof (tractors).

- Fifth wheel area, check natural compartment, skid plate (trailers).
- Exterior, front/sides (trailers).
- Rear, bumper/doors (trailers).
- Front wall (trailers).
- Left side (trailers).
- Right side (trailers).
- Floor (trailers).
- Ceiling/roof (trailers).
- Inside/outside doors and locking mechanisms (trailers).
- Outside/Undercarriage (trailers).

Conveyances and IIT (as appropriate) must be equipped with external hardware that can reasonably withstand attempts to remove it. Doors, handles, rods, hasps, rivets, brackets, and all other parts of a container's locking mechanism must be fully inspected to detect tampering, and any hardware inconsistencies prior to the attachment of any sealing device.

Visible pest contamination found during the conveyance/IIT inspection must initiate washing, vacuuming, and be carried out to remove such contamination. Documentation detailing inspections must be retained for one year to demonstrate compliance with these inspection requirements.

Inspections of conveyances and IIT must be systematic, and wherever possible conducted at conveyance storage yards. Where feasible, inspections should be conducted upon entering, and departing the storage yards, and at the point of loading/stuffing. Security inspections should be performed in an area of controlled access and, if available, monitored via a CCTV system.

The inspection of all conveyances, and IIT should be documented including the following elements on a checklist:

- Container/trailer/instruments of international traffic numbers.
- Date of inspection.
- Time of inspection.
- Name of employee conducting the inspection.
- Specific areas of the instruments of international traffic that were inspected.

If the inspections are supervised, the supervisor should also sign the checklist. If applicable, the completed container/IIT inspection sheet should be included as part of the shipping documentation packet. The consignee should receive the complete shipping documentation packet prior to receiving the merchandise.

Based on risk, management should conduct random searches of conveyances after the transportation staff have conducted conveyance/IIT inspections. Inspections may also be conducted at various locations where the conveyance is susceptible: the carrier yard, after the truck has been loaded, and en route to the destination border?

Written high security seal procedures must be in place that describe how seals are issued, and controlled at the facility, and during transit. These procedures need to provide the steps to take if a seal is found to be altered, tampered with, or has the incorrect seal number, and to include documentation of the event, communication

protocols to partners, and investigation of the incident. The findings from the investigation of a seal abnormality must be documented, and any corrective actions implemented as quickly as possible.

Written seal controls must include the following elements:

- Management of seals is restricted to authorized personnel, and is in secure storage.
- Inventory of seals, receipt of new seals, distribution of seals, and tracking of seals is recorded in a seal log, and only trained, authorized personnel may affix seals to instruments of international traffic (IIT).
- When picking up sealed IIT (or after stopping), verify the seal is intact with no signs of tampering.
- Confirm the seal number matches what is noted on the shipping documents.
- If a load is examined breaking the original seal, record the replacement seal number. The driver must immediately notify their dispatch when a seal is broken, indicate who broke it, and provide the new seal number. The carrier must immediately notify the shipper, broker, and importer of the seal change, and the replacement seal number. The shipper must note the replacement seal number in the seal log.
- Any seal discovered to be altered, or tampered with must be held to aid in the investigation. Investigate the discrepancy, follow-up with corrective measures (if warranted), and as applicable, report compromised seals to CBP, or other appropriate government agencies (if outside the U.S.) to aid in the investigation.

All shipments for importation, or exportation that can be sealed must be secured immediately after loading/stuffing/packing by the responsible party (e.g. the shipper, or packer acting on the shipper's behalf) with a high security seal that meets or exceeds the most current International Standardization Organization (ISO) 17712 standard for high security seals. Qualifying cable, and bolt seals are both acceptable. They must be securely and properly affixed to IIT that are transporting business partners cargo to, or from the United States.

C-TPAT's seal verification process must be followed to ensure all high security seals (bolt/cable) have been affixed properly to IIT, and are operating as designed. The procedure is known as the VVTT process:

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

Document that the high security seals either meet or exceed the most current ISO 17712 standard. Digital photographs of the affixed seal can be taken at the point of stuffing. To the extent feasible, these images can be electronically forwarded to the destination for verification purposes.

Seal numbers can be electronically printed on the bill of lading, or other shipping documents. Seal numbers assigned to specific shipments should be transmitted to the consignee prior to departure.

Company management, or a security supervisor must conduct audits, and inventory of seals that includes periodic inventory of stored seals, and reconciliation against seal inventory logs, and shipping documents. Dock supervisors, or warehouse managers must periodically verify seal numbers used on conveyances, and IIT.

All conveyance, and IIT procedures must be reviewed at least once a year, or more often as situations dictate, and updated as necessary. These procedures must be maintained at the local, operating level so that they are easily accessible.

A mechanism should be in place to work with transportation providers to track conveyances from origin to final destination point. Specific requirements for tracking, reporting, and sharing of data should be incorporated within terms of service agreements with service providers.

If a credible, or detected threat to the security of a shipment, or conveyance is discovered, business partners in the supply chain that may be affected, and any law enforcement agencies must be alerted as soon as feasibly possible.

Agricultural Procedures

Depending on the business partners business model (type) written procedures must be in place that are designed to prevent visible pest contamination to include compliance with Wood Packaging Materials (WPM) regulations. These measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15).

Visible pest prevention measures must be adhered to throughout the supply chain. Cargo staging areas, and the immediate surrounding areas, must be inspected on a regular basis to ensure these areas remain free of visible pest contamination.

Physical Security

Physical barriers, and/or deterrents must be in place to prevent unauthorized access to offices, trailer yards, cargo handling and storage facilities.

Perimeter fencing, if used, should enclose the areas around cargo handling and storage facilities. If a facility handles cargo, interior fencing should be used to secure cargo, and cargo handling areas. Based on risk, additional interior fencing may be required to segregate various types of cargo such as domestic, international, high value, and/or hazardous materials. Fencing should be regularly inspected for integrity, and damage by designated personnel. If damage is found in the fencing, repairs should be made as soon as possible.

Gates where vehicles, and/or personnel enter, or exit (as well as other points of ingress/egress) must be manned, or monitored.

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

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

Security Technology should be utilized to monitor the premises, and prevent unauthorized access to sensitive areas. Cameras, and recording equipment should be used to monitor the facility's premises, and sensitive areas to deter unauthorized access. Alarm systems should be used to alert of unauthorized access into sensitive areas.

If relying on security technology for physical security, written policies, and procedures must exist governing the use, maintenance, and protection of this technology. At a minimum, do these policies and procedures stipulate:

- How access to the locations where the technology is controlled/managed, or where its hardware (control panels, video recording units, etc.) is kept, and that it is limited to authorized personnel.
- The procedures that have been implemented to test/inspect the technology on a regular basis.
- That the inspections include verifications that all of the equipment is working properly, and if applicable, that the equipment is positioned correctly.
- That the results of the inspections. and performance testing is documented.
- That if corrective actions are necessary, these are to be implemented as soon as possible, and that corrective actions were taken, and documented.
- That the documented results of these inspections be maintained for a sufficient time for audit purposes.

Security technology policies, and procedures must be reviewed, and updated annually, or more frequently, as risk or circumstances dictate.

If a third-party central monitoring station (off-site) is utilized, the business partner must have written procedures stipulating critical systems functionality, and authentication protocols such as (but not limited to) security code changes; adding, or subtracting authorized personnel; password revisions(s), and systems access or denial(s).

Only licensed, or certified resources should be utilized when considering the design, and installation of security technology.

All security technology infrastructure must be physically secured from unauthorized access. Security technology systems should be configured with an alternative power source that will allow the systems to continue to operate in the event of an unexpected loss of direct power.

Camera systems where deployed, should have an alarm, or notification feature, which would signal a "failure to operate/record" condition. The cameras must be positioned to cover key areas of facilities that pertain to the import/export process. Camera systems should be programmed to record at the highest picture quality setting reasonably available, and be set to record on a 24/7 basis. The recordings of footage covering key import/export processes should be maintained for a sufficient period of time to allow an investigation to be completed for a monitored shipment. Periodic, random reviews of the camera footage must be conducted (by management, security, or other designated personnel) to verify that cargo security procedures are being properly followed in accordance with law. The results of the reviews must be summarized in writing to include any corrective actions taken, and maintained for a sufficient time for audit purposes.

Access Controls

Written procedures must exist governing how identification badges, and access devices (keys, key cards, etc.) are granted, changed, and removed. Where applicable, is a personnel identification system must be in place for positive identification and access control purposes. Access to sensitive areas must be restricted based on job description or assigned duties.

Removal of access devices must take place upon the employee's separation from the company.

Visitors, vendors. and service providers must present photo identification upon arrival, and be issued temporary identification that is it visibly displayed at all times during the visit. A registration log must be maintained that records the details of the visit including the following:

- Date of the visit.
- Visitor's name.
- Verification of photo identification (type verified such as license or national ID card).
- Time of arrival.
- Company point of contact (person being visited).
- Time of departure.

Visitors should be escorted at all times, and should not have access to sensitive areas.

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

Drivers delivering or receiving cargo must be positively identified before cargo is received, or released. They must present government-issued photo identification to the facility employee granting access to verify their identity. If presenting a government-issued photo identification is not feasible, the facility employee may accept a recognizable form of photo identification issued by the highway carrier company that employs the driver picking up the load.

A cargo pickup log must be kept to register drivers, and record the details of their conveyances when picking up cargo? When the drivers arrive to pick up cargo at a facility, a facility employee must register them in the cargo pickup log. Upon departure, the drivers are logged out. The cargo log must be kept secured, and the drivers not allowed access to it. The cargo pickup log should have the following items recorded:

- Driver's name.
- Date of Arrival.
- Time of arrival.
- Employer.
- Truck number.
- Trailer number.
- Time of departure.
- The seal number affixed to the shipment at the time of departure?

Arriving packages, and mail should be periodically screened for contraband before being admitted.

If security guards are used, work instructions for security guards must be contained in written policies and procedures.

Management must periodically verify compliance, and appropriateness with these procedures through audits and policy reviews.

Personnel Security

Written procedures for screening prospective employees, and for performing checks on current employees must exist. Application information, such as employment history, and references, need to be verified prior to employment to the extent possible, and allowed under the law. In accordance with applicable legal limitations, and the availability of criminal record databases, employee background screenings should be conducted including verification of the employee's identity, and criminal history that encompasses city, state, provincial, and country databases. Results of background checks should be factored in to hiring as permitted by local statutes in making hiring decisions.

Based on the sensitivity of the position, employee vetting requirements should extend to temporary workforce and contractors.

Once employed, periodic reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.

An Employee Code of Conduct that includes expectations, and defines acceptable behaviors must be part of policy. Employees, and contractors are required to acknowledge that they have read, and understand the Code of Conduct.

Education & Training

One of the key aspects of a security program is training. Security training, and an awareness program must be in place, and maintained to recognize, and foster awareness of the security vulnerabilities to facilities, conveyances, and cargo at each point in the supply chain which could be exploited by terrorists or contraband smugglers.

Employees who understand why security measures are in place are more likely to adhere to them. Security training must be provided to employees, as required based on their functions, and position, on a regular basis. Newly hired employees must receive this training as part of their orientation, and job skills training. This training program needs to be comprehensive and, cover all of business partner's, and governing authority's security requirements.

Personnel in sensitive positions must receive additional specialized training geared toward the responsibilities that the position holds.

Refresher training must be conducted periodically, as needed after an incident, or security breach, or when there are changes to company procedures.

Training documentation must be retained, such as training logs, sign in sheets (roster), or electronic training records. Training records should include:

Date of the training.
Names of attendees.
Topics of the training.

Measures should be in place to verify that the training provided met all training objectives.

Drivers, and other personnel that conduct security, and agricultural inspections of empty conveyances, and IIT must be trained to inspect their conveyances/IIT for both security, and agricultural purposes. Inspection training must include the following topics:

- Signs of hidden compartments.
- Concealed contraband in naturally occurring compartments.
- Signs of pest contamination.

Employees must be trained on how to report security incidents and suspicious activities.

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.

Relevant personnel must be trained on how to identify information in shipping documents, such as manifests, that might indicate a suspicious shipment.

As applicable based on their functions, and/or positions, employees must be trained on the company's cybersecurity policies, and procedures, including the need for employees to protect passwords, or passphrases, and computer access.

Employees operating, and managing security technology systems must receive training in the operation, and maintenance of these systems. Prior experience with similar systems is acceptable. Self-training via operational manuals, and other methods is also acceptable.

Cybersecurity

Comprehensive written cybersecurity policies, and/or procedures must be in place to protect information technology (IT) systems. Written IT security policy at a minimum must cover all of the individual cybersecurity criteria listed below.

Cybersecurity policies, and procedures must be reviewed annually, or more frequently as risk, or circumstances dictate. Following the review, policies, and procedures must be updated if necessary.

If a data breach occurs, or an event results in the loss of data, and/or equipment, procedures must include the recovery (or replacement) of IT systems, and/or data?

Cybersecurity policies should address how information is shared on cybersecurity threats with the government, and other business partners.

Policies, and procedures must be in place to prevent attacks via social engineering.

Cybersecurity policies, and procedures should include measures to prevent the use of counterfeit, or improperly licensed technological products.

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.

To defend Information Technology (IT) systems against common cybersecurity threats, sufficient software/hardware must be installed for the protection from malware (viruses, spyware, worms, Trojans, etc.), and an internal/external intrusion detection system must be installed (firewalls).

Security software must be current, and receive regular security updates.

When utilizing network systems, the security of the IT infrastructure must be regularly tested. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.

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

Media, hardware, or other IT equipment that contains sensitive information regarding the import/export process must be accounted for through regular inventories. When disposed of, they must be properly sanitized, and/or destroyed in accordance with the National Institute of Standards and Technology (NIST (US)) Guidelines for Media Sanitization, or other appropriate industry guidelines.

If employees are allowed 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.

Individuals with access to 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.

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.

When users are allowed to remotely connect to a network, secure technologies must be employed, such as virtual private networks (VPNs), to allow employees to access the company's intranet securely when located outside of the office. Procedures must be in place that are designed to prevent remote access from unauthorized users.