SATELLITE LOGISTICS GROUP, INC.
SUPPLY CHAIN SECURITY – BEST PRACTICES

SLG Distribution Center – Outbound Shipments

EFFECTIVE 03/09/2012

The Satellite Logistics Group (SLG) is seeking to enhance supply chain security throughout the domestic and international supply chains. It is well recognized that the two most vulnerable nodes in any supply chain occur at point of loading, and during the movement of cargo from point of loading to place of export, which includes point of U.S. egress, intermediate domestic destination, or final domestic destination. Accordingly, SLG seeks to adopt stronger security measures particularly at these two critical junctures. SLG is committed towards validating enhanced security measures which have been implemented at these most important nodes in the supply chain. Therefore, appropriate security measures, as listed throughout this document, must be implemented and maintained throughout SLG's Distribution Center (DC) supply chains.

BUSINESS PARTNER REQUIREMENTS

DC's must have written and verifiable processes for the screening and selection of its business partners, including but not limited to, contractors, carriers, and vendors. DC will review the performance of these service provider companies to detect weakness or potential weaknesses in security. Likewise, SLG will periodically review DC's processes to detect weaknesses in security.

SECURITY PROCEDURES

• Point of Origin – DC must ensure that both the DC and its business partners develop security processes and procedures consistent with the SLG security guidelines herein to enhance the integrity of the shipment at point of origin.

• Service Provider Screening and Selection Procedures – DC must have documented service provider screening and selection procedures to screen contracted service providers 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 utilize a risk-based process as determined by an internal management team.

CONTAINER/TRAILER SECURITY

DC should ensure that DC and all contracted service providers have procedures in place to maintain container/trailer integrity. Container/trailer integrity must be maintained to protect against the introduction of unauthorized material and/or persons. At point of loading, procedures must be in place to properly seal and maintain the integrity of the shipping containers/trailers. A high security seal must be affixed to all loaded containers/trailers. All seals must meet or exceed the current PAS ISO 17712 standards for high security seals as approved by SLG.

• Container/Trailer Inspection – procedures must be in place to verify the physical integrity of the container/trailer structure prior to loading, to include the reliability of the locking mechanisms of the doors. An inspection process is recommended for all containers/trailers prior to loading: front wall, left side, right side, floor, ceiling/roof, inside/outside doors, outside/undercarriage.

• 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/trailers to not only SLG but to the appropriate authority, including but not limited to, local law enforcement, federal law enforcement, & US Customs & Border Protection. Only designated employees should distribute and affix container seals for integrity purposes.

• Container/Trailer 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.

CONVEYANCE SECURITY

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

• Conveyance Inspection Procedures – 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 should be conducted at the truck yard and after the truck has been loaded, and en route to the place of export for DC's providing transportation services.

• Container/Trailer Security – for all container/trailers in the DC's custody, trailer integrity must be maintained to protect against the introduction of unauthorized material and/or persons. DC must have procedures in place to maintain the integrity of their trailers at all times and to "exercise control" over the loading of containers/trailers and the contents of the cargo. The DC must be vigilant to help ensure that the merchandise is legitimate and that there is no loading of unauthorized merchandise at the loading dock facility. For DC's providing transportation services, the DC must ensure that while in transit to the place of export, no loading of unauthorized merchandise has occurred, even in regards to unforeseen vehicle stops or trailer drops before final place of export. When the DC is loading or transporting a container/trailer, a high security seal as approved by SLG that meets or exceed the current PAS ISO 17712 standards for high security seals must be utilized. Clearly written procedures must stipulate DC's container/trailer security. These written procedures should be briefed to all DC personnel and there should be a mechanism to ensure that these procedures are understood and are being followed. These procedures must also include:

- At a minimum, DC photographs the rear of the loaded container/trailer contents and is retained by the DC.
- Container/trailer doors are to be closed and sealed upon completion of loading. The container/trailer is to be secured in a manner that precludes opening of the container/trailer door without physically moving the container/trailer.
- Secure the container/trailer until container/trailer until DC or authorized carrier departs DC with container/trailer.

• Conveyance Tracking and Monitoring Procedures – DC's providing transportation services must ensure that conveyance and container/trailer integrity is maintained while the conveyance is en route transporting cargo to the place of export by utilizing a tracking and monitoring activity log or equivalent technology. If driver logs are utilized, 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 and container/trailer pickup, point of export, and any delivery destinations, during peak and non-peak times. Drivers should notify the dispatcher of any route delays due to weather, traffic and/or rerouting. Under no circumstance is the conveyance to be detached from the underlying power unit while in transit. Likewise, equipment shall not be left unattended while in transit. DC management must perform a documented, periodic, and unannounced verification process to ensure the logs are maintained and 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 to the DC, who in turn will notify SLG, of any anomalies or unusual structural modifications found on the conveyance.

• Container/Trailer Seals – the sealing of containers/trailers, to include continuous seal integrity, are crucial elements of a secure supply chain, and remains a critical part of a DC's commitment to SLG. A high security seal must be affixed to all loaded containers/trailers departing the DC. All seals must meet or exceed the current PAS ISO 17712 (For example: Tydenbrooks International II) standards for high security seals and be approved by SLG. Clearly defined written procedures must stipulate how seals in the DC's possession are to be controlled. These written procedures should be briefed to all DC personnel and there should be a mechanism to ensure that these procedures are understood and are being followed. These procedures must include:

- Placement of the seal on the container/trailer immediately upon completion of loading and after closing of container/trailer doors only by authorized personnel with specific and approved access to seals.
- The application of the seal on the container/trailer door shall be validated on the bill of lading by two (2) DC employees, one of which is a authorized personnel.
- Verify the seal number is the same as stated by the DC on the shipping document and that the seal is properly affixed to the container/trailer door locking mechanism.

- DC shall maintain a "seal log" documenting all original and replacement seal numbers, container/trailer number, and the DC authorized personnel affixing and validating the seal number.
- For DC's providing transportation services, if the seal is removed in-transit to the point of export, even by government officials, a replacement seal must be placed on the trailer, and the seal change must be documented.
- The DC driver must immediately notify the dispatcher that the seal was broken, by whom, and the number of the replacement second seal that is placed on the trailer.
- The DC must make immediate notification to SLG of the placement of the second seal.
- Seal number and placement of seal shall be verified and recorded by the DC security at time of container/trailer departure.
- DC's will be required to submit seal usage records to SLG seal control person monthly and SLG shall reconcile the seal log with actual seal inventory.

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 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 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 upon arrival 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 and/or unidentified persons.

• Drivers, visitors and/or individuals making pickups and/or deliveries shall not have access to the DC dock area unless accompanied by authorized personnel. Restricted areas shall be clearly identified by the DC to control unauthorized access to the Distribution Center.

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, position held and submit such information to SGL 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 from the premises 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 the cargo shipped, procedures must be in place to ensure that information conveyed to business partners is reported accurately and timely.
• Shipping – departing cargo should be checked against packing lists or delivery orders. Drivers receiving cargo must be positively identified before cargo is released.
• Inventory Discrepancies – all shortages, overages and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. DC provider must notify SLG for all discrepancies, and the appropriate law enforcement agencies if illegal or suspicious activities are detected.

SECURITY TRAINING AND THREAT AWARENESS

As a liaison between SLG and the trade community, the DC should create opportunities to educate those in the supply chain they do business with on SLG policy, and those areas in which the DC has relevant expertise, which might include security procedures, best practices, access controls, documentation fraud, informationsecurity, 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 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 employee response and reporting procedures the company has in place to address a security situations they may likely encounter. 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 must have physical barriers and deterrents that guard against unauthorized access. DC must incorporate the following SLG physical security initiatives throughout their supply chains as applicable.
• Fencing – perimeter fencing shall 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 – 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 shall 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 and Video Surveillance Cameras – monitored alarm systems and video surveillance cameras shall be utilized to secure premises and prevent unauthorized access to cargo handling and storage areas.
• Local police are to provide random surveillance of the facility during non-business hours.
If for any reason the facility is NOT gated and guarded, the trailer/container must be controlled during the loading process or while in loaded status with either a pin lock or glad hand lock applied to the trailer/container. In addition, the trailer/container is to be secured in a manner that precludes opening of the trailer/container door without physically moving the trailer/container.

After normal business hours, all loaded trailers/containers must be controlled within an area that is both gated and guarded. If the DC is not configured to provide this level of security, pending over the road dispatch, subject trailer/container must be moved to an intermediate staging area that provides both gated and guarded security. In all cases, whether trailer/containers are at SLG facilities or intermediate staging areas, surveillance cameras shall be in place monitoring a single point of egress.
No loaded trailers/containers will be stored at the facility over the weekend unless the facility including any facility staging area is both gated and guarded and/or the trailer/container is locked within the facility structure itself (this security requirement may require accelerated cut off times for end of week loading).
In all cases the SLG seal protocol will be adhered to regarding the administration of trailer/container seals.

SELF AUDIT SECURITY ASSESSMENT
On a semi-annual basis all SLG warehouse facilities shall complete a security self-assessment form as cited in Exhibit A. In response, the SLG warehouse audit team shall review this assessment during physical audits of facilities to be conducted no less than on a quarterly basis. Any discrepancies shall be immediately reported to the Director of Operations for further review, evaluation, and corrective action.