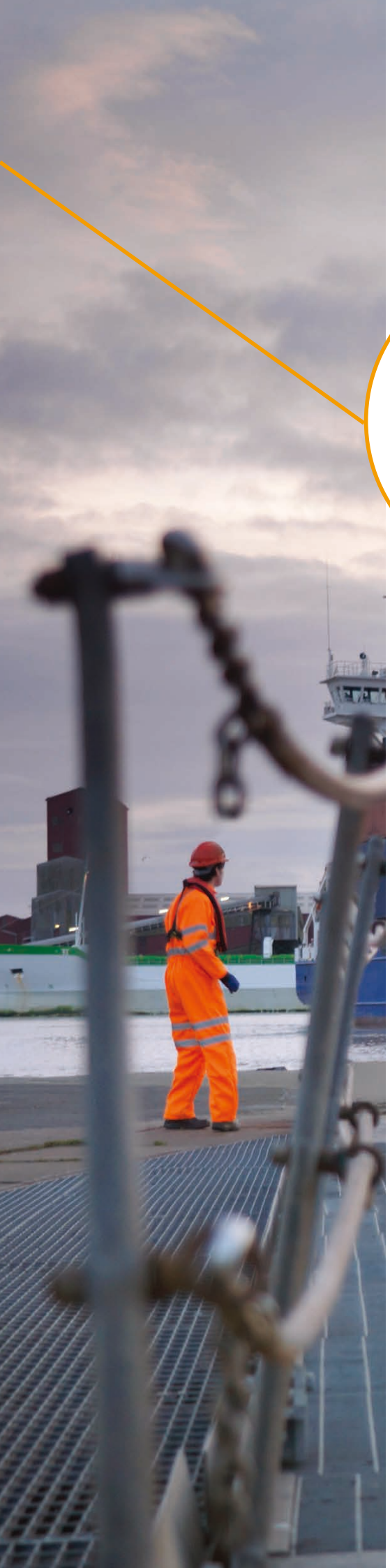
Global Security Verification (GSV) Standard

Version 1 August 2012

Intertek

Valued Quality. Delivered.

Your Perfect Solution to Enhanced Supply Chain Security



Global Security Verification (GSV) Standard

Contents

ABOUT THE STANDARD

The Global Security Verification (GSV) Standard is a program established by Intertek to help importers as well as suppliers in assessing their security measures based on international supply-chain security requirements.

OBJECTIVES AND SCOPE

In view of the escalating threat from global terrorism and piracy, governments and customs organizations around the world have implemented supply-chain security standards to secure trade flows, protect against terrorist acts, and to combat illegal trafficking.

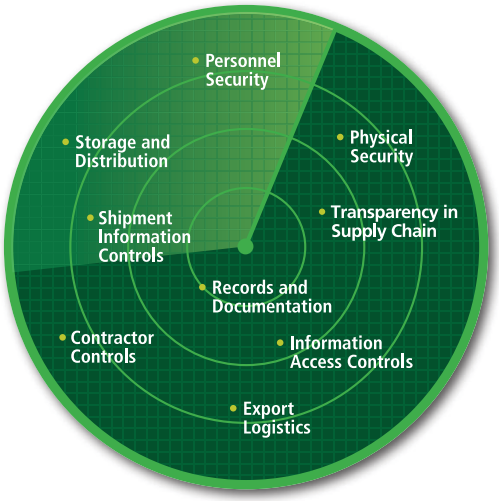
In the process of enforcing and adhering to new international supply-chain security standards, companies must assess their supply chain to identify, mitigate and eliminate all potential security risks.

Intertek's Global Security Verification program integrates multiple global suplly-chain security initiatives, including C-TPAT (Customs Trade Partnership Against Terrorism), PIP (Partners in Protection) and AEO (Authorized Economic Operators). Our mission is to partner with international buyers and suppliers to drive the development of a global security-verification process, resulting in increased safety assurance, risk control, efficiency and cost savings for all participants.

The Global Security Verification Standard includes:

9 Security Modules

1. Records and Documentation
2. Personnel Security
3. Physical Security
4. Information Access Controls
5. Shipment Information Controls
6. Storage and Distribution
7. Contractor Controls
8. Export Logistics
9. Transparency in Supply Chain



BENEFITS

- Saving time and money by undergoing few security andits
- Saving cost and time and reducing business disruptions by facilitating quicker customs clearance through GSV which is well recognized
- Enhancing reputation with a world-recognized program that confirms compliance with global supply chain criteria
- Enabling importers and suppliers to leverage efforts through a common industry platform and collaboration
- Engaging with a Global Security Program which covers best practice from C-TPAT, PIP & AEO

SUMMARY OF THE "GLOBAL SECURITY VERIFICATION" CRITERIA

Section	Sub-Section
1. Records and Documentation	1.1 Records and Documentation
2. Personnel Security	2.1 Documented Personnel Security Policies/ Procedures 2.2 Personnel Screening 2.3 Identification System 2.4 Education/ Training/ Awareness
3. Physical Security	3.1 Plant Security 3.2 Perimeter Security 3.3 Outside Lighting 3.4 Container Storage 3.5 Security Force 3.6 Access Controls 3.7 Visitor Controls 3.8 Entering/ Exiting Deliveries 3.9 Employee/ Visitor Parking 3.10 Production, Assembly, Packing Security
4. Information Access Controls	4.1 Information-Access Controls
5. Shipment Information Controls	5.1 Shipment-Information Controls
6. Storage & Distribution	6.1 Storage 6.2 Loading for Shipment
7. Contractor Controls	7.1 Contractor Controls
8. Export Logistics	8.1 Export Logistics
9. Transparency in Supply Chain	9.1 Transparency in Supply Chain

RESOURCES / REFERENCES

Minimum security criteria for foreign manufacturers

DEFINITIONS

- Contractors - "Contractors" refer to business partners of a facility, including other subcontracted manufacturers, product suppliers, and vendors, as well as service providers, e.g., catering, security guards, computer/ office-machine maintenance, cleaning staff, repairmen, etc.
- 3PL – Third Party Logistics

The Global Security Verification Criteria Implementation Guidance

The following sections give an explanation of the Global Security Verification Criteria and provide guidance on what a supplier needs to do to develop, document, and implement the criteria.

1.1 RECORDS AND DOCUMENTATION

Intent

Measures must be in place to ensure the integrity and security of processes throughout the supply chain and a written policy has to be established stipulating all security procedures that need to be documented.

Program Requirements	Implementation / Indicators for Achieving Compliance
Facility has a policy that requires that all security procedures be documented	- A written policy shall be established by the facility stipulating all security procedures that need to be documented
Facility has a security department/ personnel and has designated a security chief	- A person or department responsible for security of the facility. The facility has designated a company official responsible for: ◦ Plant security ◦ Personnel security ◦ Contractor security ◦ Conveyance/ Transport security ◦ Security audits or evaluations
Facility has conducted a site security assessment	- Internal security audit performed by facility or second- or third-party security assessment (e.g., GSV)
Facility has documented procedure to conduct periodic security checks to ensure that the security procedures are being performed properly	- A documented procedure for conducting an internal security audit which includes the following: ◦ Personnel Security ◦ Physical Security ◦ Information Access Control ◦ Shipment Information Controls ◦ Storage and Distribution ◦ Contractor Controls ◦ Export Logistics
Facility has documented security improvement action plan summarizing identified vulnerabilities and their relevant corrective	- A documented improvement plan from completed assessments/ audits, and evidence that the plan is reviewed by management and security departments periodically

Good Practices

- Internal security audit every three months for high-risk countries and every twelve months for medium-risk countries.
- Security plan is reviewed every six months for high-risk countries and every twelve months for medium-risk countries.

2.1 DOCUMENTED PERSONNEL SECURITY POLICIES/ PROCEDURES

Intent
A documented process must be in place to screen prospective employees in order to evaluate risk associated criminal records, drug usage or other security related risk.

Program Requirements	Implementation / Indicators for Achieving Compliance
Facility has written personnel security guidelines for hiring	- A written guideline or procedure for personnel security, which includes procedures for hiring employees, employee-identification system, and employee-access control
Security guidelines for hiring are evaluated periodically to ensure their effectiveness	- Factory evaluates the personnel security guidelines
Written personnel security guidelines and requirements are being applied to contracting temporary and part time employees	- The documented personnel security guidelines that apply to the hiring of contracted, temporary, and part-time employees are the same as those that apply to the hiring of full-time employees

Good Practices
• Hiring guidelines to be evaluated every six months to ensure their effectiveness.

2.2 PERSONNEL SCREENING

Intent
A process must be in place to screen prospective employees and obtain application information, such as employment history and references that are verified prior to employment. In addition, periodic background checks of current employees holding sensitive positions should be consistently conducted.

Program Requirements	Implementation / Indicators for Achieving Compliance
Employment applications are required of applicants	- Employment applications required
Facility has a process for interviewing applicants	- Applicants interviewed

Program Requirements	Implementation / Indicators for Achieving Compliance
Background checks are conducted on all applicants	- Application information, such as employment history and references, are verified prior to employment - Background checks and investigations conducted for prospective employees, consistent with national regulations which may include: ◦ Criminal record checks ◦ Employment history checks ◦ Reference checks ◦ Drug test
Facility has a process for examining and verifying an applicant's official identification	- Examine and verify the applicant's official identification
Periodic and follow-up background checks are conducted on employees based on circumstances and/ or sensitivity/ scope of employee responsibility	- Periodic follow-up background checks conducted on employees based on circumstances and/ or sensitivity/ scope of employee responsibility
Facility maintains a permanent employee personnel file for each employee	- Personnel file maintained for each employee which includes the full name, date of birth and the national identification number of the employee

Good Practices
• Criminal background check and drug test.

2.3 IDENTIFICATION SYSTEM

Intent
Identification system must be in place for employees for positive identification and access-control purposes for identified restricted areas.

Program Requirements	Implementation / Indicators for Achieving Compliance
Company identification is required for entry of personnel	- A company ID like card key (IC card) or company badge is required for the employees to enter into facility - Newly hired employees should have temporary passes - Company ID that cannot be easily tampered or duplicated
Security guards monitor employee arrival at the facility for positive identification to ensure that only those with a company issued ID badge are allowed entry	- Presence of security guard or personnel at employee entrance who checks ID of incoming employees

Program Requirements	Implementation / Indicators for Achieving Compliance
Identification has unique identifiers	- The ID includes a biometric indicator, i.e. a unique physical identifier such as a facial photograph or fingerprint
The issuance of employee identification is centralized and controlled by a specific department	- A designated department (e.g. human resources or admin department) in facility to issue, retrieve and control the employee's ID - The related written procedure or the record for issuance of employee ID shows that it is centralized and controlled by a specific department
The control over distribution and inventory of employee ID badges and facility access keys/ cards/ codes is restricted to a limited number of authorized employees	- Identification of authorized employees who can issue the IDs, keys, cards and codes
Documented procedures and records in place for employees to return their IDs when they leave the facility permanently	- Procedures that include those employees are required to return their badges when they leave the company - Record to support the return of badge after employees resign and leave from company
Documented Employee Termination policy and procedures in place to retrieve IDs and deactivate access as needed	- Procedures for the issuance, removal, and changing of access devices (e.g., keys, key cards) must be documented - Procedures in place to retrieve IDs and/ or deactivate access as needed
A list of terminated employees is given to security to deny access to facility	- List of terminated employees issued to security department or security guards. - Facility must be able to demonstrate that access has been terminated such as posted notice in the main entrance
Lost IDs are replaced and recorded as missing in the employee's personnel file before a replacement badge is issued	- Procedures for the issuance, removal, and changing of access devices (e.g., ID access cards) must be documented - Lost ID record or similar records showing the missing ID are replaced and recorded as missing such as letter or affidavit from employees stating that their IDs were lost or application for replacement
Lost or stolen keys are replaced and recorded as missing and/ or is reported immediately to the factory management	- Procedures for the issuance, removal, and changing of access devices (e.g., keys, key cards) must be documented - Records showing reported missing keys and key replacement
The security staff informed of such losses (name, ID number, etc) to prevent unauthorized use	- The security staff are informed of missing IDs through records or written notice

Program Requirements	Implementation / Indicators for Achieving Compliance
IDs are required to access restricted areas	- Restricted areas defined by facility and normally includes cargo handling such as packing, finished goods warehouse, loading areas, IT room, etc. - IDs specify access for loading/packing dock areas by any or combination of the following: ◦ Color Coding ◦ Numeric Coding ◦ Map Coding ◦ Electronic Coding - Where restricted areas exist, guards or system are adopted to check employee IDs to monitor access to these areas

Good Practices

- Facility-employee identification centralized and controlled by a specific department.
- Guards monitor access to the restricted areas by checking employee IDs.
- Posted signs stating "Restricted Areas - For Authorized Personnel Only".
- Records maintained of all persons entering a restricted area.

2.4 EDUCATION / TRAINING / AWARENESS

Intent
Employees must be made aware of the security procedures the company has in place to address a situation and how to report a security incident. Additional specific training should be provided to employees to assist them in maintaining cargo integrity, recognizing internal conspiracies, and protecting access controls. A threat-awareness program should be established and maintained and should offer incentives for active employee participation.

Program Requirements	Implementation / Indicators for Achieving Compliance
Facility requires new employee orientation	- New employee orientation training records and training materials that includes: ◦ Confirming that all onsite personnel are wearing IDs at all times while in the facility premise ◦ Challenging and reporting unidentified persons to security or management personnel ◦ Recognizing internal conspiracies ◦ Detection of unlawful activities ◦ Maintaining cargo integrity ◦ Computer security ◦ Reporting compromised security infrastructure (broken locks, windows, computer viruses, etc.) ◦ Recognizing and detecting dangerous substances and devices
Facility has written security awareness program covering awareness of current terrorist threat(s), smuggling trends, and seizures in place to ensure employees understand the threat posed by terrorist at each point of the supply chain	- The facility has a security awareness program in place and requiring all personnel to participate and maintaining training plan and records - Periodic security program update training required every six months for high-risk countries and twelve months for medium risk-countries and records maintained - Methods for increasing security awareness such as posters, e-mail bulletins, newsletter, stickers, meetings, certifications, e-learning tools and TV ads are all effective tools for creating an environment in which employees actively participate in keeping the workplace secure

Program Requirements	Implementation / Indicators for Achieving Compliance
	- Threat awareness training program includes training and encouraging personnel to report irregularities, suspicious activity and/ or security violations and procedures used by the facility to resolve the situation through use of suggestion box, phone number or hotline - Incentives are used as a method to encourage personnel in reporting irregularities. The incentive portion of the requirement is intended to be a positive reward to encourage people to participate in security controls beyond the basic expectations for personnel to abide by company security rules. Incentives may be low or no cost or something with monetary value such as: ◦ Public notoriety for participation in security controls (e.g., recognition in staff meetings, or printed in company newsletters/ periodicals) ◦ A certificate for participating in security training ◦ A reserved parking stall for a period of time for suggesting ideas to improve security - Cash (or equivalent) awards for reporting illegal activity or for making a suggestion relating to security that saves the company money and/ or reduces security vulnerabilities
Facility has a process in place to publicize the security procedures throughout the facility	- Documented security procedures publicized throughout the facility i.e. posters, bulletin boards, media wall, publications

Good Practices

- Employees are encouraged to report irregularities through incentives.
- Facility maintains an employee code of conduct such as an employee handbook.

3.1 PLANT SECURITY

Intent
Facility premise should be monitored and secured to prevent unauthorized access to restricted and cargo-handling/ storage areas. All buildings must be constructed of materials that resist unlawful entry.

Program Requirements	Implementation / Indicators for Achieving Compliance
The facility has intrusion detection or alarm system	- Automatic intrusion-detection or alarm system installed at least in sensitive/ controlled access areas and/ or perimeter fence and barrier. (Intrusion alarm is a system that gives sound alert when an opening such as door, gate or window is opened without proper access) - Alarm system is tested regularly and has a back-up power source for the alarm system - Records showing that intrusions are reported
Locking devices secure facility access points and are used to control access to restricted areas	- Locking devices protect ◦ External doors ◦ Internal doors ◦ Windows ◦ Gates - Locking devices activated through use of: ◦ Key ◦ Card ◦ Code ◦ Others - Locking devices are in working order and are inspected regularly and inspection records are maintained
Facility has key control program that establishes an individual responsible for distributing and maintaining keys/ cards	- Written key control program includes issuing record shows the keys, codes, cards are distributed by individual person(s) - Key control program includes a control log that accounts for all keys/ access cards on-hand, issued, and returned (name, date out, date in, reason, name of issuing person) - A monthly record of the inventory of the facility's access keys, codes, cards to employees is maintained - Approved list of employees with special access to controlled or sensitive areas
When an employee leaves the company, keys/ cards are returned and codes are changed and a record is maintained of these actions	- Written termination procedure to remove identification of facility (e.g., company badge) and system access (IC card access right) for terminated and resigned employees or employees transferred to another position - Records of returned keys/ cards and deactivation of codes

Program Requirements	Implementation / Indicators for Achieving Compliance
Buildings must be constructed of materials that resist unlawful entry	- Production buildings and warehouses should be constructed of durable and impenetrable materials that prevent unlawful entry and to protect against outside intrusion - The buildings are properly maintained and repaired so that there are no open areas through floors, roof or broken walls - Records of building infrastructure integrity (including inspection dates, reported damages, and completed repairs) are maintained

Good Practices
• Facility management reviews and approves a list of employees with special access to controlled or sensitive areas every month for high risk countries and every three months for medium risk countries.

3.2 PERIMETER SECURITY

Intent
Facility should be secured with perimeter fencing or physical barriers and deterrents and should enclose areas around cargo-handling and storage facilities that guard against unauthorized access. Gates used for entry should be manned and/ or monitored.

Program Requirements	Implementation / Indicators for Achieving Compliance
The perimeter of the property is secured	- Physical barriers surround and secure the perimeter of the property to deter unauthorized access with: ◦ Chain-link fence ◦ Masonry or concrete wall ◦ Steel wall ◦ Electric fence ◦ Concertina wire - The facility perimeter is secured with a sturdy fence or wall, and/ or is patrolled by security guards, to deter unauthorized access - The requirement of height of the perimeter is two meters (eight feet) or sufficient to deter easy entry
The perimeter barrier and gates regularly inspected to check for damage and attempted illegal access, properly maintained and repaired	- Perimeter fencing inspection records or similar showing that all fencing and gate must be inspected for integrity and damage on daily basis for high-risk countries and weekly basis for medium-risk countries

Program Requirements	Implementation / Indicators for Achieving Compliance
The perimeter barrier and gates are properly maintained and repaired	- Fenced areas maintained to prevent illicit entry via any adjoining/ overhanging structures or foliage, or additional security monitoring is provided. (Adjoining structures are: trees near the walls; parked containers near the walls; roof of neighboring company which is the same level and attached to the wall; elevated water tanks with ladder near the wall; or any structure that can be used as entry to the perimeter fence) - Underground access points, culverts, utility tunnels, sewers, including manholes and drainage secured to prevent unauthorized access
Entrances/ exits for the facility are secured by gates	- All gates are manned and/ or monitored - Only facility management and designated security guard supervisor have keys or other controls necessary to open/ close facility gates

Good Practices

- Facility management and designated security-guard supervisor only have keys or other controls necessary to open/ close facility gates.

3.3 OUTSIDE LIGHTING

Intent

Adequate lighting must be provided outside the facility, including at entrances/ exists, cargo-handling/ storage areas, fence lines, and parking areas.

Program Requirements	Implementation / Indicators for Achieving Compliance
The facility has outside lighting and the entire perimeter of the facility (including gates) is lighted	- Adequate lighting inside and outside the facility, including around entrances and exits, cargo-handling and storage areas, fence lines and parking areas - The lighting system has an emergency power source/ generator - Access to the lighting switches restricted to only authorized personnel - During darkness, the facility perimeter fence/ wall is well lit

Good Practices

- Access to the lighting switches restricted to authorized personnel only.

3.4 CONTAINER STORAGE

Intent
Containers must be stored in a secure area to prevent unauthorized access and/ or manipulation and to ensure the integrity of cargo. Container storage areas should be enclosed with perimeter fencing.

Program Requirements	Implementation / Indicators for Achieving Compliance
The loaded stored containers/ trailers are sealed with high security seals that meet or exceed ISO/ PAS 17712 standard	- Containers must be stored in a secure area to prevent unauthorized access and/ or manipulation - Unloaded containers should be parked with the doors facing each other (In small companies, if this is not possible, where only one container can be stored in the facility, the door ends should face the loading dock) - Doors of the containers should be closed and locked if there is no loading activity
Containers are stored in a designated container storage area surrounded by a secure fence or wall	- Containers or trailers should be placed well away from the perimeter fence otherwise they could constitute adjoining structures that might enable unauthorized entry into the facility - The container storage area is surrounded by a secure fence or wall
Facility has documented procedures in place for reporting and neutralizing unauthorized entry to container storage areas	- Documented procedure in place

Good Practices
• Container/ trailer-storage area surrounded by a secure fence or wall.

3.5 SECURITY FORCE

Intent
The facility should have a designated security guard force that monitors and secures the facility and aims to identify, challenge, and address unauthorized/ unidentified persons and stops introduction of illegal materials.

Program Requirements	Implementation / Indicators for Achieving Compliance
Facility has a designated security guard force	- A security guard force or other employee(s) who undertake similar functions such as walk-through to monitor the appropriate implementation of security processes, supervising the unloading/ loading of containers, monitoring access to restricted areas, registering visitors/ trucks, etc.
Security supervisor/ guards log incidents	- The records of the security guard should log incidents or daily issues while the security guard is on duty
Security guards report incidents related to compromised seals and/ or containers/ trailers to appropriate local authorities	- Procedure or instruction that customs and/ or other appropriate law enforcement agencies are notified if illegal or suspicious activities are detected, as appropriate (The incidents related to cargo security, broken seal, etc.) - Security guards job description that includes procedure on how illegal or suspicious activities should be reported to local authorities
Security guards should report any security-violation incidents, including tampering involving a loaded or empty container/ trailer to management personnel	- Incident log or written procedure showing that the guard reported the incidents to management personnel - Number of management personnel should be available to the guard to report emergency cases - Security guards job description that includes procedure on how illegal or suspicious activities should be reported to the management
Available communication system between the central security office and the exterior guard posts	- Internal communications system in place to contact security personnel such as walkie-talkie or two-way radio and mobile phones
Guards receive specific security training	- Specific training should be offered to guard or security personnel in maintaining cargo integrity, recognizing internal conspiracies, and protecting access controls; training materials and records are maintained, and should include: ◦ Terrorism threat awareness ◦ Unauthorized access ◦ Internal conspiracy ◦ Firearm handling (if required by law) ◦ Customs-Trade Partnership Against Terrorism (C-TPAT) or other security standard awareness such as PIP (Partners in Protection), AEO (Authorized Economic Operator) - Periodic refresher and/ or update training material and records

Program Requirements	Implementation / Indicators for Achieving Compliance
Facility has proper communication mechanism to local law enforcement authorities	- Internal communications system in place to contact security personnel and/ or local law enforcement - The communications system should be functional even under difficult or unexpected circumstances. For example: ◦ facilities should have several standard phones that do not rely on electric power to function ◦ facilities should have back-up batteries for prolonged use of walkie-talkie and mobile phones

Good Practices
• The facility should have a designated security guard force that staffs the facility 24 hours a day, 7 days a week (24/7).

3.6 ACCESS CONTROLS

Intent
Access controls must be in place to identify, challenge, and address unauthorized/ unidentified persons which includes the positive identification of all employees, visitors, and vendors at all entry points.

Program Requirements	Implementation / Indicators for Achieving Compliance
Gates for employees and vehicle entrances/ exits must be guarded and/ or monitored during operating hours and during non-operating hours	- Gates should be secured with any of the following: ◦ Guards at the gate ◦ Patrolling guards ◦ CCTV ◦ Motion detector
Employees' entries and exits must be logged	- Time keeping system for entry and exit to facility
Employees must be observed and/ or subject to security inspection when entering the building	- Checking of belonging, body frisk, magnetometer screening
Guards should patrol the interior of the facility buildings	- The guard on duty patrol inside buildings during operation and/ or non-operation hours
Closed circuit television cameras (CCTVs) should be used to monitor activity in the facility, including fence/ wall and entrance gates	- Video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to cargo handling/ storage areas - Cameras located in cargo handling/ packing areas - Positioning of the cameras should provide adequate views of activities in relevant areas

Program Requirements	Implementation / Indicators for Achieving Compliance
CCTV recordings (e.g., tapes or electronic files) should be kept for a minimum of 30 days or according to client's specific requirements, whichever is longer	- All video surveillance recording must be continuous or motion detection activated, 24 hours a day, 7 days a week - Recorded surveillance images must be stored for at least 30 days or according to client's requirement whichever is longer - Recordings could be through PC hard disk, network folders, CD, VCR or other means
CCTVs monitored	- Availability of staff to monitor the real-time activities captured by CCTV constantly on all shifts preferably by full-time security personnel with no other duties - CCTV monitor is in secured and controlled area

Good Practices

- Gates locked and/ or monitored during non-operating hours by Patrolling Guards and CCTV.
- CCTVs monitored and access to CCTV monitors controlled.

3.7 VISITOR CONTROLS

Intent

Visitor access controls must be in place which includes procedure for positive identification of all visitors and vendors at all entry points and monitoring visitors activities by escorting them or limiting their access if possible.

Program Requirements	Implementation / Indicators for Achieving Compliance
Same security control points applied to employees and visitors when entering and exiting the factory	- Some examples of same control points are: ◦ Regulating the movement of people (employees, visitors, vendors) to meet the operational and security needs of the facility ◦ Verifying authenticity of ID ◦ No ID, no entry ◦ Body frisk, bag and belonging inspection, inspection of vehicles
Advance information from a vendor required before the visit	- Relevant record showing the notification in advance of visit with visitor name, company representing, date and time of arrival, purpose of visit
Facility maintains up-to-date list of names and addresses of all contractor (e.g., canteen staff), vendor, repair personnel	- A list of all contractor (if applicable), vendor, and repairmen (if applicable) and must include the name and address - The security guard house or the point of visitor access should maintain an up-to-date list

Program Requirements	Implementation / Indicators for Achieving Compliance
Photo identification required of all visitors	- The visitors are required to show the identification document with photos (such as driver license, company ID with photo, national ID etc.)
A positive identification process for recording all vendors and repair personnel and facility have a written procedure to challenge, identify, and remove unauthorized/ unidentified persons	- Access controls must include the positive identification of all visitors, and vendors at all entry points - For deliveries, proper vendor ID and/ or photo ID must be presented documentation purposes upon arrival by all vendors - Written procedures in place to challenging, identifying, and removing unauthorized/ unidentified persons - Authorized employee nominated to supervise contractors while at the facility - All visitors escorted and monitored while accessing facility specifically on restricted areas (e.g., loading/ unloading, IT, finance)
Visitors log maintained	- Visitors' log maintained includes recording date and time of entries and/ or exits, visitor's name, purpose of visit and escort name
Visitors (including contractors) required to wear temporary ID badges	- All visitors should wear visibly displayed temporary ID - The visitor badge shall have numbering/ coding - If reusable visitors badge is used, it should be tamper proof such as bearing company logo with original signature of management representative and laminated - The visitor badge issue/ return should be controlled by the issue/ return log which could be combined together with visitor registration logbook

Good Practices

- Same security control points applied to employees and visitors when entering and exiting the factory.
- Advance information from a vendor required before the visit, including visitor name, company representing, date and time of arrival, purpose of visit.

3.8 ENTERING / EXITING DELIVERIES

Intent
Arriving goods, packages and mail should be periodically screened before being distributed and drivers delivering/ receiving cargo must be positively identified before cargo is received/ released.

Program Requirements	Implementation / Indicators for Achieving Compliance
Documented procedures implemented to periodically screen arriving packages and mail prior to distribution	- Detailed procedure on how mails and packages are being screened and checked for security prior to distribution - In most cases, a policy is documented that all mails and packages will be screened
Both incoming and outgoing cargo vehicles checked	- Inspection of incoming and outgoing goods whether loaded in containers, trailers or trucks done by security staff
Advance notice required for a pick-up or delivery transport company	- Record of notice from forwarder, trucking or 3PL including driver name, company, date and time of arrival and purpose of trip
Conveyance drivers required to show positive identification	- Positive ID can include the National ID cards, driver license, company badge, etc. - Conveyance driver should show the ID at the entrance every time when they pick-up or deliver the cargo, regardless of their frequency of visiting the facility - Information of personal ID (e.g. ID number, employees' number, etc.) should be recorded in the cargo vehicles in-out log or similar record
Conveyance drivers required to show a truck manifest upon entry and/ or exit	- Records of manifest check or information available
Cargo log in and out maintained	- The log at the point of the entering/ exit (gate) includes: ◦ Truck license ◦ Driver's name ◦ Time and date of entry/ exit ◦ Manifest check ◦ Container number ◦ Name of guard ◦ Seal number
Full incoming and outgoing containers and/ or trailers sealed	- A record showing the seal is inspected when containers or trailers are entering/ leaving the faciltity - A record showing the seal number is recorded when containers or trailers are entering/ leaving the faciltity

Program Requirements	Implementation / Indicators for Achieving Compliance
Documented procedure for handling cases of broken seals	- Records of actual reported broken seal case (if any) - Documented procedure includes that broken seals immediately reported to security, local law enforcement and/ or customs authorities (as relevant) and to facility management - Documented procedure includes that when broken seals (including cargo hold locks) are discovered, there is an examination of the container's/ trailer's/ trucks'/ closed van's contents - Documented result of examinations which includes overage/ shortages and other type of anomalies - Documented procedure includes that broken seal is immediately replaced on outgoing container's/ trailer's/ trucks'/ closed van's contents and new seal number is recorded
Documented procedure to verify seal and seal number	- Documented procedure to verify seal number against facility documentation and whether the seal is intact when the container/ trailer is turned over to the next supply chain link (applicable to trucks and closed vans)
Shipping/ receiving parking lots separated from all other parking lots	- The parking lot for the truck, container, trailer etc should be separated from other parking like employees or visitor private car parking - The shipping/ receiving parking lots are not mixed with employees or visitor parking lots - "No Parking for Private Vehicles" signage

Good Practices
• Seals on incoming containers/trailers are inspected and seal numbers recorded.

3.9 EMPLOYEE / VISITOR PARKING

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

Program Requirements	Implementation / Indicators for Achieving Compliance
Vehicles prohibited/ prevented from parking near cargo conveyances	- Private passenger vehicles must be prohibited from parking in or adjacent to cargo-handling and storage areas - At the parking lots for cargo conveyance and cargo handling & storages areas, warning sign(s) are posted to prohibit/ prevent other vehicles from parking near by
Vehicles prohibited/ prevented from parking near the perimeter fencing	- Warning sign posted near the perimeter fencing which prohibits the vehicles from parking near the perimeter
If allowed to enter the facility area, vendor and visitor vehicles should be inspected prior to admission	- General inspection such as visual inspection of inside of car and use of under mirror for under the vehicle
Visitor and employee personal-vehicle parking lots should be monitored by security guards during facility operating hours	- Parking lots include the employees parking and visitor parking - Monitoring means observed by guards or have the CCTV coverage/ monitored
Facility require the use of visual identification for visitor and employee parking	- Use of visual identification for parking - Visual identification means the coded parking sticker, tag, decal or cards which are issued by facility and placed on the visitor vehicle for identification

Good Practices
• If available, the parking lots for visitors should be separated from those for employees. • Visitor and employee parking lots should be located away from entrances and exits.

3.10 PRODUCTION, ASSEMBLY, PACKING SERCURITY

Intent
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.

Program Requirements	Implementation / Indicators for Achieving Compliance
Security measures in place to prevent tampering of goods during production	- The security measures for preventing the tampering of goods during production including CCTV monitoring, workers are observed by line supervisor, security guard patrol, etc. - Some examples: ◦ Production lines are monitored by CCTV ◦ Workers are observed by line supervisor ◦ Production lines are patrolled by security personnel
Security measures in place to prevent the introduction of foreign material(s) into the assembly area and packing area	- Facility has clear access control system in such area and has the policy prohibiting the employees to carry the foreign material(s) into the packing area - Providing lockers for employees' personal belongings before their entry is one of the security measures which is acceptable
Procedures for detecting and reporting shortages and overages	- Documented procedure in place

Good Practices
• Locker areas separated from production area.

4.1 INFORMATION-ACCESS CONTROLS

Intent
Documentation control must be implemented that includes safeguarding computer access and information and procedures in place to ensure that all information used in clearing merchandise/ cargo is legible, complete, accurate, and protected against the exchange, loss, or introduction of erroneous information.

Program Requirements	Implementation / Indicators for Achieving Compliance
Procedures for identifying which employees are allowed access to computers and information	- Documented procedures for identifying those employees who are allowed access to: ◦ Electronic information systems ◦ Facility documents ◦ Shipping forms ◦ Shipping data ◦ Shipping/ cargo movement ◦ High security seals
Controlled access to the server room	- Server is secured in a room that requires special access and monitored
Electronic information systems password protected	- Automated systems must use individually assigned accounts that require a periodic change of password - Password changes required by policy or enforced in a systematic manner at least every six weeks for high-risk countries and eight weeks for medium-risk countries - The change of password is forced by computer setting or forced by the procedural system with supporting document provided (The system/ server setting should be capable to show that the password needs to be changed regularly)
Facility have procedures to adjust or rescind such access	- Relevant written procedure addressing the adjust or rescind of access right of computer user - Login user ID suspended after three failed access attempts - Desktops automatically locked after a designated period of inactivity
Facility has designated system administrator	- The system administrator is responsible for: ◦ Setting up individually assigned IT system accounts and passwords of relevant employees ◦ Receives and reviews a daily report of invalid password attempts and file access ◦ Conducts meetings with senior management to review system security concerns

Program Requirements	Implementation / Indicators for Achieving Compliance
A system in place to identify IT abuses, including improper access, tampering, or the altering of business data	- System includes firewall, virus protection and intrusion warning system - Documented procedures for investigating violations and disciplining IT system violators, as appropriate
All computer information saved on a back-up system	- The facility should back up data in order to ensure that records still exist even if the main IT system is disabled (virus attack, fire at the factory, etc.) through hard disk, CD, back-up server, etc. - Back-ups stored in a fire-resistant safe or at an off-site facility (Off site could be outside of the facility or another building inside the facility; back-up records can be outside the IT room such as the General Manager's room but should be in a fire-proof vault) - Established written plan to restore data in the case of a failure

Good Practices
• Desktops automatically lock after a designated period of inactivity.

5.1 SHIPMENT-INFORMATION CONTROLS

Intent
All information used in clearing merchandise/ cargo is legible, complete, accurate, and protected against the exchange, loss, or introduction of erroneous information and procedures must be in place to ensure that information provided by the company is reported accurately and timely.

Program Requirements	Implementation / Indicators for Achieving Compliance
Facility has designated company representative responsible for shipment information control	- The designated company representative is responsible for: ◦ Providing accurate information on the facility's products to the broker/ forwarder ◦ Providing accurate information on the facility's products to the carrier - The designated company representative has been trained on the information requirements for shipments to the applicable country - The responsible company representative understand the need to provide accurate shipper, forwarder, and consignee information - The responsible company representative understand the timeframes required for the advance information
Records maintained on all shipments for at least twelve months	- Shipment records maintained on all shipments for at least twelve months
Facility conducts a review of shipment information and documentation controls to verify accuracy and security	- Records of review of shipment information at least every three months for high-risk countries and at least every six months for medium-risk countries

Good Practices
• Automation of information requirements

6.1 STORAGE

Intent
Containers are stored in a secure area to prevent unauthorized access and/ or manipulation.

Program Requirements	Implementation / Indicators for Achieving Compliance
Doors secured for empty stored containers/ trailers	- Where there is no loading activity, the container doors should be locked at all times - Partially loaded containers must be closed when employees are taking their breaks - Doors can be secured by using lock, bar-type container intrusion device, high-security seal, etc.
Facility uses fencing or other barrier materials to enclose cargo handling and storage areas to prevent unauthorized access	- Cargo handling and storage areas secured with perimeter walls, fencing or other barrier materials to prevent unauthorized access
Dangerous cargo, including hazardous materials, ammunition and explosives, secured and stored separately	- Interior fencing within a cargo handling structure should be used to segregate hazardous cargo - Dangerous cargo are labeled when necessary
High value cargo marked, segregated and stored separately within a fenced area or secured room	- Interior fencing within a cargo handling structure should be used to segregate high value cargo
International and domestic cargo segregated and stored separately within a fenced area or secured room	- Interior fencing within a cargo handling structure should be used to segregate domestic and international cargo

Good Practices
• High-value cargo marked, segregated, and stored separately within a fenced area or secured room.

6.2 LOADING FOR SHIPMENT

Intent
Control and security measures must be in place to ensure the integrity and security of processes relevant to the handling, storage, loading and transportation of cargo in the supply chain including verifying the physical integrity of the container structure and reliability of door-locking mechanisms prior to stuffing.

Program Requirements	Implementation / Indicators for Achieving Compliance
Loading and departure of containers /trailers are supervised by a security officer or other designated supervisor	- A supervisor and/ or security personnel should observe all loading and unloading activities in order to ensure that the actual product count is exactly the same as reflected on the shipping papers
Loading and departure of containers/ trailers is captured on CCTV and the recording is kept for forty-five days	- CCTV records capturing the loading and departure of containers, trailers, trucks and closed vans
Shipping area and loading dock access restricted to authorized personnel only	- The loading area shall be restricted and the process must be in place to identify, challenge, and address unauthorized/ unidentified persons - Sign of "Authorized Person Only" at the loading dock area
Security controls in place, to prevent the introduction of foreign material(s) or non-manifested items at point of loading, and to prohibit employees bringing in their personal items into the shipping area	- Only authorized cargo and personnel is allowed in the loading area. Employees are not permitted to bring into the loading area their personal items such as lunch box, backpack, ice container/ water cooler - Facility has clear access control system in such area and has a policy (e.g. a sign posted at loading area) of prohibiting the employees to carry the foreign material(s) into the loading area
Cargo moved directly from the storage facility/ assembly line to the conveyance without intermediate staging	- The packing area and loading area should be closed off to all transit activities and transfer of finished goods should be without intermediate staging
Documented and implemented procedures to ensure that accurate, legible, and complete cargo documents and packing slips prepared	- Procedures must be in place to ensure that all information used in the clearing of merchandise/ cargo, is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous information - Export or shipping records should be legible, complete and accurate. - Documents are prepared electronically
Documented system in place to ensure that management, customs and/ or local law are informed of and investigates all anomalies found in shipments and/ or the accompanying documents	- Documented procedure in place for reporting anomalies found in cargo and shipment information documentation
Procedures for tracking goods for shipment	- Written procedure showing the tracking of goods for shipment such as "Outbound Shipment Procedure"
Cargo verification procedure in place to prevent non-manifested cargo from being loaded	- Written procedure related to cargo verification before loading - Procedure should include that all product counts conducted by at least two persons to ensure accuracy - A loading checklist is another tool to promote product count accuracy

Program Requirements	Implementation / Indicators for Achieving Compliance
Detect and report cargo shortages and overages during container/ trailer loading, and ensure cargo is identified and labeled, weighed, and counted before loading	- Related records showing the cargo units are weighed and carton boxes were identified or labeled such as packing list and loading checklist
All containers checked for tampering, false compartments, and other evidence of unauthorized access before loading	- Related records showing the container/ truck are checked for tampering, false compartments, and other evidence of unauthorized access
Procedures in place to verify the integrity of the container structure through 7-point inspection	- Documented 7-point inspection procedure, include: ◦ Front wall ◦ Left side ◦ Right side ◦ Floor ◦ Ceiling/ roof ◦ Doors ◦ Undercarriage - Related records showing 7-point container inspection kept for forty-five days and records indicate when modifications have been made to the container - Training record in-charge for conducting the inspection - Actual demonstration of 7-point container inspection of the assigned personnel
All trailers checked for tampering, false compartments, and other evidence of unauthorized access before loading	- Documented 15-point inspection procedure for non-refrigerated trailer, include: ◦ Bumper ◦ Engine ◦ Tires (trailer and truck) ◦ Truck floor ◦ Cab/ storage compartments ◦ Air tanks ◦ Drive shafts ◦ Fifth wheel ◦ Front wall ◦ Side walls ◦ Trailer floor ◦ Ceiling/ roof ◦ Inside/ outside walls ◦ Undercarriage - Documented 17-point for refrigerated trailer and tractor inspection, include: ◦ All 15-point inspection procedure ◦ Refrigerated unit ◦ Exhaust

Program Requirements	Implementation / Indicators for Achieving Compliance
	- Related records showing 15-point trailer inspection kept for 45 days and records indicate when modifications have been made to the trailer - Training record in-charge for conducting the inspection - Actual demonstration of 15-point trailer inspection of the assigned personnel
Security personnel performs truck outbound inspection	- Documented procedure and records of truck inspection that includes verifying that the transportation document is complete, indicates the departing container/ trailer number, and verifies that the actual security seal number is the same seal number listed on the shipping document
Procedure to affix a high-security seal which meets or exceeds ISO/ PAS 17712 on each container/ trailers bound for the US	- Documented procedure to affix an ISO/ PAS 17712 seals
ISO/ PAS 17712 compliant high security seals used on each outbound container/ trailers	- The facility needs to provide the written certificate/ test report to prove high security seals are ISO/ PAS 17712 compliant
Procedures for affixing, replacing, recording, and tracking the seals placed on containers, trailers, trucks, and/ or railcars	- Written procedures must stipulate how seals are controlled, affixed and tracked to loaded containers, trailers, trucks and/ or railcars
For pick-ups from multiple manufacturers, the facility requires transportation providers to use secure locking devices (e.g., padlocks) for less-than-full-load containers	- The facility has the related document like carrier procedure, contract etc stating that the transportation providers to use locking devices for less-than-full-load container
There is designated individual responsible for issuing, accessing and tracking seals	- Identified authorized personnel through memo, announcement, job description, etc.
Unused seals kept in a locked cabinet and access restricted to authorized employee(s)	- Physical storage of unused seals and measures must be in place to access the storage
Outgoing cargo verified against transportation/ shipping document before departure and facility keep records of verification	- Verification records or seal control log includes the following information: ◦ Truck license ◦ Driver name ◦ Time and date of loading or unloading ◦ Container/ cargo conveyance number ◦ Seal number with name of person using the seal and date of use of seal
Trucks sealed as soon as loading is complete	- Photos of sealing or seal records and transport information
Seal numbers verified at time of final sealing before departure	- Verification of seal numbers should be stipulated in procedure, implemented and recorded

Good Practices

- Cargo moved directly from the storage facility/ assembly line to the conveyance without intermediate staging.
- All documents prepared electronically.
- For pick-ups from multiple manufacturers, the facility requires transportation providers to use secure locking devices (e.g., padlocks) for LCL (less-than-full-load) containers.

7.1 CONTRACTOR CONTROLS

Intent
Facility must have written and verifiable processes for the selection of business partners such other manufacturers, product suppliers, service suppliers and vendors (parts and raw material suppliers, etc.).

Program Requirements	Implementation / Indicators for Achieving Compliance
The facility should have a verifiable process for selecting contractors	- "Contractors" refer to business partner of facility including other subcontracted manufacturer, product suppliers, vendor as well as the services provider (e.g., catering, security guards, computer/office machine maintenance, cleaning staff, repairmen) - Written records like "Contractor Selection Record" or similar records show the contractors are selected according to security controls, financial stability, corporate history and hiring practices
Written security standards and documented procedures for selection of contractors (contracts, manuals, etc.)	- Written security standards and documented procedures for selection of contractors according to security controls, financial stability, corporate history and hiring practices - Written contractor procedures include security standards for the contractor's employees while at the facility
Contractors with access to restricted areas should undergo a background investigation	- Record of background investigation for contractor or contractor's employees
Facility or third party auditor conduct on-site inspections of the contractors' implementation of the above standards/ procedures	- Audit reports of contractor assessments. - Communication history for the schedule of assessments and request for corrective action
Facility requires its contractors to conduct self-assessment of their security policies and procedures and share the results of those assessments with the facility	- Completed self-assessment forms of contractors - Communication history for completing self-assessments
Contractors retained through legally binding contracts	- Signed service contract agreements

Good Practices
• Facility requires Customs-Trade Partnership Against Terrorism (C-TPAT) enrollment of its contractors or other relavent security standards such as PIP (Partners in Protection) or AEO (Authorized Economic Operator).

8.1 EXPORT LOGISTICS

Intent
Facility must have written and verifiable processes for the selection of carriers and other Third-Party Logistics (3PL) providers and ensuring that eligible partners are certified and ineligible partners are compliant with the international security standards or its equivalent.

Program Requirements	Implementation / Indicators for Achieving Compliance
Facility select the land carriers, sea carriers, rail carriers, consolidators, freight forwarders, NVOCCs (Non-Vessel Operating Common Carriers), or other third party logistics providers hired to transport goods	- A verifiable process of hiring and selecting the carriers - Written records like "Carrier Selection Record" or similar records show the carriers are selected according to security controls, financial stability and corporate history - Proof of client nomination - Selection process should include considering carriers: ◦ Security control ◦ Financial stability ◦ Corporate history ◦ C-TPAT (Customs Trade Partnership Against Terrorism), AEO (Authorized Economic Operators), PIP (Partners in Protection) and other equivalent standards certification or implementation
Facility requires eligible carriers to demonstrate C-TPAT, AEO, PIP certification and/ or ineligible carriers to demonstrate compliance with C-TPAT, AEO, PIP equivalent standards	- For eligible carriers, any evidence that facility is requiring the carriers to provide their eligibility such as C-TPAT, AEO, PIP certificate or Status Verification Token is acceptable showing facility name and SVI (Status Verification Interface) - Eligible Carriers for C-TPAT member: ◦ U.S./ Canada Highway Carriers ◦ U.S./ Mexico Highway Carriers ◦ Rail Carriers ◦ Sea Carriers ◦ Air Carriers ◦ Third Party Logistics Providers (3PL) ◦ Long Haul Highway Carriers in Mexico - Proof of nomination by C-TPAT member US importers - For non-eligible carriers, any evidence that facility is participating compliance with C-TPAT requirements such as second and third party audits - Third Party Logistics Provider Eligibility Requirements. In order to be eligible for participation in the C-TPAT program, the 3PL must: ◦ Be directly involved in the handling and management of the cargo throughout any point in the international supply chain, from point of stuffing, up to the first U.S. port of arrival (Entities which only provide domestic services and are not engaged in cross border activities are not eligible)

Program Requirements	Implementation / Indicators for Achieving Compliance
	◦ Manage and execute these particular logistics functions using its own transportation, consolidation and/ or warehousing assets and resources, on behalf of the client company ◦ Does not allow subcontracting of service beyond a second party other than to other CTPAT members (does not allow the practice of "double brokering", that is, the 3PL may contract with a service provider, but may not allow that contractor to further subcontract the actual provision of this service) ◦ Be licensed and/ or bonded by the Federal Maritime Commission, Transportation Security Administration, U.S. Customs and Border Protection, or the Department of Transportation ◦ Maintain a staffed office within the United States Note: Non asset-based 3PL's who perform duties such as quoting, booking, routing, and auditing (these type of 3PL may posses only desks, computers, and freight industry expertise) but do not own warehousing facilities, vehicles, aircraft, or any other transportation assets, are excluded from C-TPAT enrollment as they are unable to enhance supply chain security throughout the international supply chain
Security measures in place when facility use in-country transport services	- In-country transport services should: ◦ Vary routes ◦ Employ security guards ◦ Require goods be transported within defined time-limits ◦ Record transport times ◦ Provide vehicle escort ◦ Use Global Positioning Satellite (GPS) ◦ Use truck convoys ◦ Document procedure to report security violations to facility management ◦ Require that the driver report any incident of attempted cargo theft, load tampering, or other security violations
Security measures in place when facility use carrier services	- Carrier has intermediate staging/ rest period/ layover of cargo conveyances prior to reaching the consolidation center/ port/ border
Written or electronic confirmation of partners' compliance with C-TPAT or C-TPAT-equivalent security criteria	- Contract language, a letter of commitment signed at management level or above, signed acknowledgement of receiving the facility's C-TPAT participation announcement
Facility has written legal contract with a transport company who moves a container/ trailer from the facility to the next destination in the supply chain	- Signed contracts with transport company
Facility conducts a periodic unannounced security check to ensure that transport company is in compliance with the contract	- Procedures of unannounced security check are available - Records of security check kept for at least twelve months

Good Practices

- When selecting carriers, the facility considers Financial Stability and Corporate History.
- In-country transport services: vary routes, employ security guards, provide vehicle escort, use Global Positioning Satellite (GPS) and truck convoy.

9.1 TRANSPARENCY IN SUPPLY CHAIN

Intent
Efforts made by the company to evaluate and address risks of human trafficking and slavery in the supply chain.

Program Requirements	Implementation / Indicators for Achieving Compliance
System in place to ensure that management is informed of and investigates all anomalies found in shipments including human trafficking	- Documented procedure of investigation in case of slavery and human trafficking cases
Cargo verification procedure in place to prevent un-manifested cargo and/ or illegal aliens from being loaded	- Written procedure related to cargo verification before loading
Facility or a third party auditor conduct on-site inspections of the contractors' implementation of the security standards/ procedures including compliance with human trafficking and slavery policies	- Audit reports of external security and social compliance assessments which includes slavery and human trafficking and some checkpoints related to migrated workers or forced labor in social audit report
Facility requires its contractors to conduct self-assessment of their security policies and procedures including status of their compliance with human trafficking and slavery policies and share the results of those assessments with the facility	- Completed self-assessment forms of contractors which include slavery and human trafficking
facility have written or electronic confirmation of its partners' compliance with Business Transparency on Human Trafficking and Slavery Act (e.g., contract language, a letter of commitment signed at the management level or above, signed acknowledgement of receiving the facility's participation announcement)	- Certification or email confirmation with Business Transparency on Human Trafficking and Slavery Act such as contract language, a letter of commitment signed at the management level or above, signed acknowledgement of receiving the facility's participation announcement
Facility have written security standards and documented procedures for selection of its contractors (contracts, manuals, etc.) and handling contractors failing to meet company standards regarding security and slavery and trafficking	- Contractor selection procedure which includes selection of supplier who complies with Business Transparency on Human Trafficking and Slavery Act
Written security awareness program covering awareness of current terrorist threat(s), human trafficking, smuggling trends, and seizures in place to ensure employees understand the threat posed by terrorist at each point of the supply chain	- Program outline, training plan and training records - The facility has the records to show that human trafficking and slavery as a topic is included in the regular security awareness training/ briefing

APPENDIX — INTERTEK COUNTRY SUPPLY CHAIN SECURITY RISK INDEX

Country	Intertek Country Supply Chain Security Risk Index
Argentina	high
Australia	low
Austria	low
Bahrain	high
Bangladesh	high
Belgium	low
Brazil	medium
Bulgaria	medium
Cambodia	high
Canada	low
Chile	high
China	high
Costa Rica	medium
Croatia	medium
Cyprus	medium
Czech Republic	medium
Denmark	low
Dominican Rep.	medium
Ecuador	medium
Egypt	high
El Salvador	medium
Finland	low
France	low
Germany	low
Greece	medium
Guatemala	high
Haiti	high
Honduras	high
Hong Kong	medium
Hungary	low
India	high
Indonesia	high
Ireland	low
Israel	high
Italy	low
Japan	low
Jordan	high
Kenya	medium
Korea, South	medium
Kuwait	high

Country	Intertek Country Supply Chain Security Risk Index
Latvia	low
Lebanon	high
Lesotho	medium
Madagascar	high
Malaysia	high
Mauritius	low
Mexico	medium
Morocco	high
Netherlands	low
New Zealand	low
Norway	low
Pakistan	high
Panama	medium
Peru	high
Philippines	high
Poland	medium
Portugal	low
Puerto Rico	low
Romania	medium
Russia	medium
Saudi Arabia	high
Serbia	medium
Singapore	low
Slovakia	medium
South Africa	medium
Spain	low
Sri Lanka	medium
Swaziland	low
Sweden	low
Switzerland	low
Taiwan	low
Thailand	medium
Turkey	medium
Ukraine	medium
United Arab Em	high
United Kingdom	low
USA	low
Venezuela	high
Vietnam	high

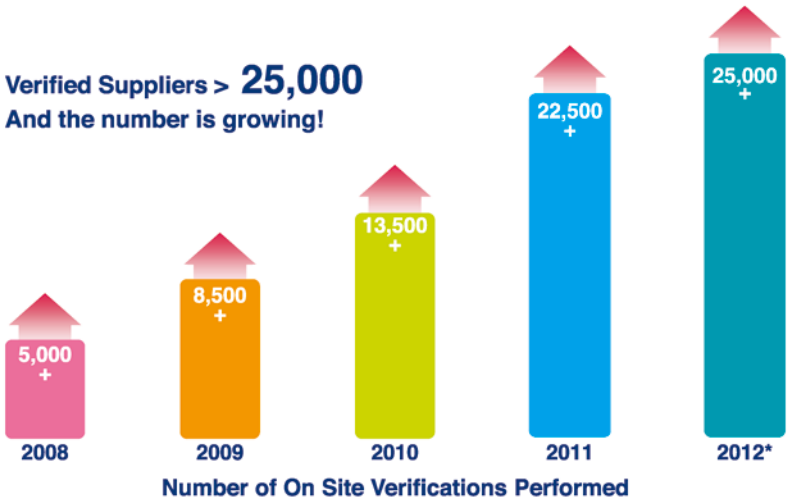
The "Intertek Country Supply Chain Security Risk Index" predicts the supply chain security risk associated with a number of parameters in each country including but not limited to:

1. Practice for cargo logistics
2. Clearance and Customs process
3. Political and economic condition
4. Historical country performance in security verifications for the last 10 years.

Program Features

▶World's Largest Community of Verified Suppliers

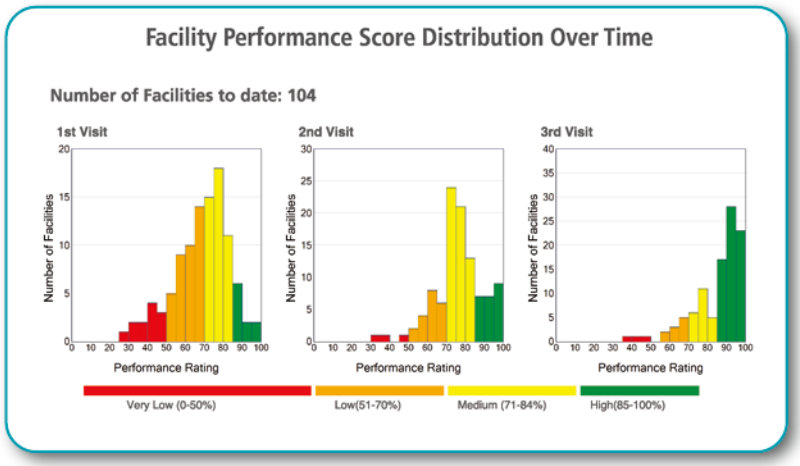
Intertek's range of Supplier Qualification Programs are the world's largest community of verified suppliers with over 25,000 participating facilities. Undertaking our qualification programs allows you to increase your facility's compliance, and map the compliance risk in your supply chain through the effective use of reports and charts to keep track of supplier performance against industry, country and global benchmarks.



*As at Mar, 2012

▶Continuous Improvement

Intertek Supplier Qualification Programs are not the traditional pass or fail audit programs. Instead, continuous improvement action is possible with constant feedback and monitoring of results. The outcomes are measurable through statistics.

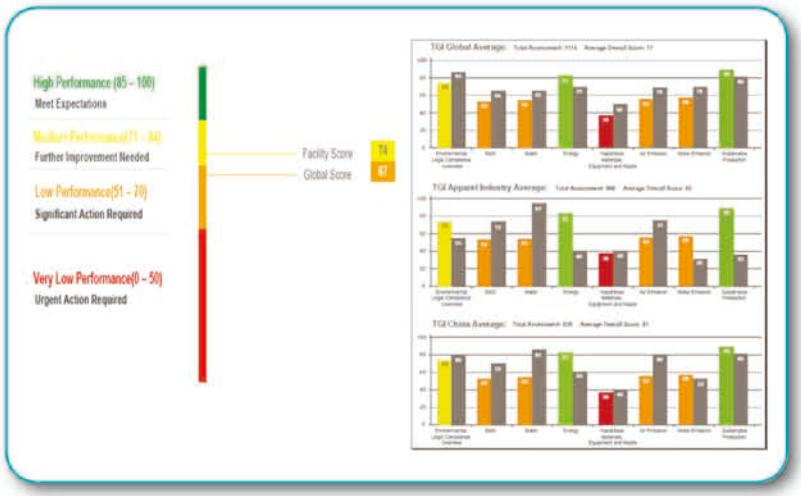


▶Data Mining

As Intertek Supplier Qualification Programs create the world's largest community of suppliers, data mining of suppliers performance is made possible. Through the detailed reports, suppliers can know their strengths and risks. Buyers can also better manage their suppliers and make more informed buying decisions.

Benchmarking

Benchmarking of supplier' performance against Country, Industry or Global averages is possible, providing suggestions on targeted improvement actions based on performance and risk factors.



Report Sharing

Suppliers and facilities can share their qualification reports with their clients, which are recognized by many of the world's leading buyers. This can help reduce audit fatigue and business disruption as suppliers and facilities do not have to complete audits for different buyers.

Suppliers and facilities share report with their clients

Achievement Award / Record of Participation

Upon satisfactory fulfillment of assessment criteria for each qualification program, the supplier or facility will receive an Achievement Award / Record of Participation (GSV Program only). The awarded suppliers or facilities can use the program logo and the Achievement Awards / Records of Participation as a valuable marketing tool to showcase their performance to buyers, and thus winning buyers' confidence.

Workplace Conditions Assessment (WCA) Achievement Award

Think Green Initiative (TGI) Achievement Award

Supplier Qualification Program (SQP) Achievement Award

Mill Qualification Program (MQP) Achievement Award

Global Security Verification (GSV) Record of Participation

This page is intentionally left blank

This page is intentionally left blank

Intertek

Valued Quality. Delivered.

Intertek is a leading provider of quality and safety solutions serving a wide range of industries around the world. From auditing and inspection, to testing, quality assurance and certification, Intertek people are dedicated to adding value to customers' products and processes, supporting their success in the global marketplace. Intertek has the expertise, resources and global reach to support its customers through its network of more than 1,000 laboratories and offices and over 30,000 people in more than 100 countries around the world. Intertek Group plc (LSE: ITRK) is listed on the London Stock Exchange and is a constituent of the FTSE 100 index.

www.intertek.com

For more information on Intertek Qualification Programs, please email to: **qualification@intertek.com**

GSV-V1-0812E