

GE Customs-Trade Partnership Against Terrorism (C-TPAT) Supply Chain Security Guidelines for International Suppliers or Shippers

To support the GE Aviation and U.S. Customs and Border Protection (CBP) C-TPAT program, our business partners (international suppliers or shippers) who handle U.S. bound shipments to GE from another country, must follow the C-TPAT security guidelines below to ensure supply chain security and mitigate the risk of loss, theft, and contraband smuggling that could potentially introduce terrorists or implements of terrorism into the global supply chain. **Contact GE Aviation hotline immediately at 513-243-2100 upon knowledge of any security breach affecting GE goods (contraband, smuggling, or threatening/suspicious activities).**

Business Partners/ Subcontractor Requirements: Foreign suppliers and shippers must have documented procedures for selection of business partners like carriers and vendors who handle (manufacture, package, or transport) U.S. bound shipments to GE. This includes evidence (e.g., C-TPAT SVI, AEO or equivalent program number and certificate) to indicate partners who are certified and compliant with C-TPAT, AEO or an equivalent supply chain security program. Foreign suppliers or subcontractors must have documentation of compliance verification (e.g., contractual obligations, certification records, or completed questionnaires).

Shipment Routing & Certified Carrier Usage: Foreign suppliers and shippers must follow GE Incoterms and instructions for delivery, routing, and international shipment. On U.S. bound GE import shipments the supplier or shipper must use C-TPAT certified forwarders and carriers. This requirement applies to subcontractors handling or transporting GE U.S. import shipments (e.g., transfer carriers for truck trailers from Mexico).

GE Importer Security Filing (ISF) Form & Pre-alert Process: For U.S. bound GE import shipments arriving by vessel, the supplier, shipper & forwarder must follow GE ISF process. The forwarder (within 72 hours prior to stuffing) must email GE ISF form and shipping documents to GE ISF agent (customs broker stated on invoice and ISF form). The broker must file ISF 10 per SOP (within 24 hours prior to vessel sailing) and email completed ISF form to forwarder and GE with ISF acceptance. After receipt of ISF acceptance, forwarder may stuff & load GE's shipment onto vessel.

Point of Origin: Point of Origin is the facility where products are assembled, manufactured, packaged, and shipped. Foreign suppliers and shippers must ensure partners have security procedures consistent with C-TPAT security criteria to enhance integrity of shipments at point of origin. Periodic reviews of partner facilities should be conducted based on risk to maintain CBP standards.

Security Procedures: Container and trailer security procedures below for inspections, storage, and seals apply when foreign suppliers or shippers are responsible contractually for stuffing or loading truck trailers and ocean containers at their facility (i.e., FCA Supplier or Shipper Facility Incoterms 2010). Suppliers and shippers must work with carriers to ensure effective security controls are implemented at point of origin.

Container and Trailer Security: Container and trailer integrity must be maintained to protect against introduction of unauthorized material and/or persons. At the point-of-stuffing, procedures are required to properly seal and maintain the integrity of shipping containers and trailers. A high security seal that meets or exceeds the current PAS ISO 17712 standard must be affixed to all U.S. destined containers and trailers.

Seven-Point Ocean Container Inspection: Procedures and checklist are required to verify the physical integrity of each ocean container and door locking mechanisms prior to stuffing. *Seven-point ocean container inspection process: (1) outside and undercarriage (before entering shipping/receiving areas), (2) inside and outside doors, (3) right side, (4) left side, (5) front wall, (6) ceiling and roof, (7) floor (inside).*

Seventeen-Point Truck & Trailer Inspection: Procedures and checklist are required to verify the physical integrity of the truck & trailer and door locking mechanisms prior to stuffing. *Seventeen point truck & trailer inspection process: (1) bumper, (2) engine, (3) tires (truck & trailer), (4) floor (inside truck), (5) fuel tanks, (6) cab*

and storage compartments, (7) air tanks, (8) drive shafts, (9) fifth wheel, (10) outside and undercarriage, (11) outside and inside doors, (12) floor (inside trailer), (13) side walls, (14) front wall, (15) ceiling and roof, (16) refrigeration unit, and (17) exhaust.

Ocean Container and Truck Trailer Storage: Ocean containers and truck trailers under the supplier or shipper control or located in a facility of the supplier/shipper must be stored in a secure area and manner to prevent unauthorized access and/or manipulation.

Security and Control of Container and Trailer Seals: For ocean containers and truck trailers fully loaded at international supplier/shipper facilities the supplier or shipper must affix a high security seal to all fully loaded ocean containers or truck trailers bound for the U.S., have documented procedures to control and record use of high security bolt seals, recognize and report compromised seals, containers or trailers, designate a limited number of employees to access/apply seals for security purposes and keep a documented inventory of all seals.

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/Access Devices: Systems are required for positive identification and access control of employees and visitors. Employees should only have access to secure areas based on their duties. Company management or security personnel must 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 and Deliveries (including mail): Visitors must present photo identification for documentation purposes upon arrival. All visitors should be escorted and should visibly display temporary identification. 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/unidentified persons.

Personnel Security: Screening prospective employees and periodic checks of current employees is required.

Pre-Employment Verification, Background Checks/Investigations: Application information like employment history and references must be verified before employment. Consistent with foreign regulations, background checks and investigations should be conducted for prospective employees. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.

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

Physical Security: Supplier/Shipper facilities must have physical security deterrents to protect from unauthorized access. Physical security deterrents used by international suppliers/shippers may include:

Fencing, Gates/Entries & Guards: Perimeter fencing or walls should enclose facilities where other controls are not in place to prevent unauthorized access. Fencing and walls should be inspected & maintained. Shipping & receiving areas should have fencing, locking doors, access controls or CCTV. Entry and exit points for vehicles and/or personnel must be controlled. The number of gates should be kept to the minimum necessary for proper access and safety controls. Guards or access controls should be in place to ensure that unauthorized personnel do not enter the facility or gain access to GE shipments.

Parking & Lighting Controls: Private passenger vehicles should be prohibited from parking in or adjacent to shipping and receiving areas to prevent unauthorized materials from being introduced into shipments or conveyance vehicles. Adequate lighting must be provided inside and outside facilities to prevent unauthorized access.

Locking Devices, Key Controls: External & internal windows, gates, and doors to access the facility or cargo storage areas must be secured with locking devices. Management or security personnel control issuance of all locks and keys.

Alarms Systems and Video Surveillance Cameras: Suppliers and shippers should use alarm systems and video surveillance cameras, as appropriate, to monitor premises and prevent unauthorized access to cargo handling and storage areas.

Information Technology (IT) Security: Security measures must be in place to ensure automated systems are protected from unauthorized access.

Password Protection & Accountability: Automated systems should use individually assigned accounts that require a periodic change of password. IT security policies, procedures and standards should be in place and provided to employees in the form of training. A system should be in place to identify the abuse of IT including improper access, tampering or the altering of business data. All system violators should be subject to appropriate disciplinary actions for abuse.

Procedural Security: Documented security procedures must be communicated to employees to ensure security measures are followed. Upon GE's request, the supplier or shipper shall provide evidence of documented procedures like physical, personnel and IT security, access controls, reporting of security incidents, ocean container or truck trailer seal and inspection controls.

Shipment Documentation and Manifesting Procedures: Procedures must ensure accurate and timely information is received from partners. Invoice, packing list, bill of lading and other records to manifest and clear cargo with Customs will be legible, complete, accurate, and protected from exchange, loss or erroneous information. Controls must include securing computer access and information.

Packing, Shipping and Receiving Security Procedures: Documented procedures must control access to shipping & receiving areas. Packaged shipments must be controlled to prevent unauthorized access and contraband. Departing cargo must be verified against purchase or delivery orders with accurate package and unit quantities weight and part numbers and verification that contraband is not present. Drivers picking up cargo should be positively identified before cargo is released. Procedures should track the timely movement of incoming and outgoing goods.

Cargo Discrepancy and Security Breach Reporting: All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. **Contact the GE Aviation hotline immediately at 513-243-2100 upon knowledge of any security breach affecting GE goods.** Notify Customs and/or other law enforcement agencies as appropriate when contraband, smuggling or threatening suspicious activities are detected. Contact your GE representative with any questions.

Security Training: A security training program must be in place to educate and build employee awareness of proper security procedures as outlined in these security guidelines including training on the threat posed by terrorists and contraband smugglers at each point in the supply chain, training on ethical conduct, avoidance of corruption, fraud and exploitation. Additional training on effective supply chain security controls should be given to employees in the shipping and receiving areas.