



C-TPAT Expectations

For Material Suppliers



For Distribution to all existing and potential Material Supplier Entities

Contents

0.	INTRODUCTION.....	2
1.0.	UPPER MANAGEMENT	2
2.0	RISK ASSESSMENT	3
3.0	BUSINESS PARTNERS	3
4.0	PROCEDURAL SECURITY.....	3
5.0	CONVEYANCE & INTERNATIONAL INSTRUMENTS OF TRAFFIC (IIT) SECURITY	4
6.0	AGRICULTURAL PROCEDURES	6
7.0	PHYSICAL ACCESS CONTROLS.....	6
8.0	ACCESS CONTROLS	7
9.0	TRAINING.....	8
10.0	CYBER SECURITY	8
11.0	PERSONNEL SECURITY	9
12.0	MATERIAL SUPPLIER ACKNOWLEDGEMENT FORM FOR SECURITY PROGRAM PARTICIPANTS	10
13.0	MATERIAL SUPPLIER ACKNOWLEDGEMENT FORM – OTHER	11
14.0	STATUS OF MRAS.....	12
15.0	CONTAINER INSPECTION FORM	13
16.0	CBP CREATED TEMPLATES FOR CONTAINER INSPECTIONS.....	14
17.0	CBP CREATED TEMPLATES FOR TRUCK AND TRAILER INSPECTIONS.....	14



0. Introduction

At GE Vernova Gas Power (GE Vernova Gas Power, GE Vernova Hitachi Nuclear and GE Vernova Renewables North America), we understand that if our supply chain were disturbed or compromised it could have a significant impact on our business and business relationships. GE Vernova Gas Power has taken steps internally to protect our supply chain and likewise, we are asking our suppliers to ensure the safety and security procedures in the following areas:

- Upper Management
- Risk Assessment
- Business Partners
- Procedural Security
- Conveyance and International Instruments of Traffic (IIT)
- Agricultural
- Physical Security
- Access Controls
- Training
- Cybersecurity
- Personnel

GE Vernova Gas Power has identified the minimum requirements for each of these specific areas of focus noted above that apply to all our suppliers who provide goods where the final destination of such goods is the U.S. We recognize that some of the requirements are based on U.S. standards and may not be possible to implement in other countries. We also recognize that certain requirements may not be appropriate for some suppliers due to size, structure, and location. However, it is important for each supplier to ensure and acknowledge that:

- security regulations are formulated and implemented to protect your company, employees, and the security of GE Vernova Gas Power's supply chain, and
- your employees observe your security policies and report any suspicious or improper actions to management and/or the proper authorities.

*If your company is certified under C-TPAT or certified under a Mutually Recognized Arrangement (MRA) please proceed to the **last page of this document and complete the Business Provider Acknowledgement Form.** – [Click here.](#)*

1.0. Upper Management

1.1 UPPER MANAGEMENT

CTPAT requires that your senior leadership is aware of the program, involved in report outs on the program, and supports the program. Your leadership must issue a statement of support signed by a senior company official and displayed in appropriate locations (internal and external web document locations).

1.2 CROSS-FUNCTIONAL REPRESENTATION

CTPAT requires companies to have a cross-functional team to cover a robust supply chain security program. All team representatives and involved points of contact must be knowledgeable with CTPAT.

1.3 WRITTEN COMPONENT REVIEW

The policies, procedures, involved parties and their responsibilities must be documented. This includes how requirements are being executed. Each Supplier must include a minimum of one annual audit as part of effective program monitoring.



1.4 SUPPLY CHAIN UPPER MANAGEMENT SUPPORT AND OVERSIGHT

Each Supplier is required to have a process where their CTPAT team provides regular reporting to their senior leadership. Regular updates need to be provided throughout the year to provide the leadership with a view of the supply chain health (audits, exercises, & validations) within the CTPAT guidelines.

2.0 Risk Assessment

2.1 OVERALL RISK ASSESSMENT OF SUPPLY CHAIN

The amount of risk in the supply chain needs to be assessed annually and documented. Supplier is required to conduct the [5-step risk assessment](#) and has developed a written procedure on how to execute the requirement. The risk assessment document must be reviewed annually, at a minimum, based on risk factors identified within this program.

2.2 DETAILED RISK POLICIES & PLANS

A written procedure must be in place to address crisis management, business continuity, security recovery plans and business resumption.

3.0 Business Partners

3.1 BUSINESS PARTNER SCREENING

Each supplier must maintain a written risk-based process for screening new business partners and for monitoring existing partners that comply with the CTPAT guidelines documented on the CTPAT site (<https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat-customs-trade-partnership-against-terrorism/apply/security-criteria>). Business partners can include: Logistics Service Providers, Direct Material Suppliers, Customs Brokers, Warehouses, etc. Screening items at a minimum include: cybersecurity, improper payments, terrorism financing, human trafficking, agricultural terrorism, organized crime, and other factors that may contribute to any of these or related risks. Additionally, partners should be screened for participation in CTPAT, Authorized Economic Operator (AEO) program, or another Mutual Recognition Arrangement (MRA) with the United States. If they do not fall into one of these categories, they must answer a series of questions to determine if CTPAT Minimum Security Criteria (MSC) are met.

3.2 REVIEW OF SHIPMENT DOCUMENTATION

The supplier involved must review import/export documentation for signs of suspicious cargo shipments including: originated from or destined to unusual locations, paid by cash or a certified check, using unusual routing methods, exhibit unusual shipping/receiving practices. The requirement can be managed by 3rd party partner, like a customs broker, provided that the supplier maintains oversight of the process. These specific 3rd party partners must ensure their employees are trained to recognize the signs.

3.3 ADDRESSING BUSINESS PARTNER DEFICIENCIES If a business partner is found to have any shortcomings during the outlined screening process from section 3.1, the participating owners must implement corrective actions and close them within a timely manner. Security, safety, quality or trade compliance related findings require immediate correction.

4.0 Procedural Security

4.1 INFORMATION & DOCUMENTATION

It is a requirement that suppliers maintain procedures that ensure information used in the clearing of merchandise/cargo must be legible, complete, accurate, protected against exchange/loss/introduction of erroneous information and reported on time. Accuracy of information includes but is not limited to: weight, piece count, first foreign location/facility where carrier takes possession, & value. The requirement for



accuracy extends to the business partner/s included in the transaction (e.g. direct material supplier, carrier, etc.).

4.2 LOGISTICS PROCESS REQUIREMENTS

Logistics teams must maintain processes pertaining to the following topics: security for cargo staged overnight or for an extended period of time, supervision of stuffing/destuffing of cargo containers/IIT, verifying departing cargo against purchase order/delivery order, reconciling arriving cargo against manifest/shipping documents with investigation/reporting/resolution of discrepancies, pre-alert is required in advance of arrival to US border.

4.3 VERIFICATION OF INFORMATION PRE-MOVE/AT-ARRIVAL

Loading/stuffing of cargo into containers/IIT should be supervised by the responsible GE Vernova supervisor, if conducted on-site. Otherwise, the business partner should execute loading/stuffing to this requirement. Arriving cargo should be verified against the manifest/invoice and any shortages, overages, significant discrepancies, or other anomalies require appropriate reporting, escalation, and resolution.

4.4 INVESTIGATIONS, REPORTING & CBP NOTIFICATION

Internal investigations must be performed immediately after an incident. Notifications of security incidents need to be reported to CBP as soon as feasibly possible and in advance of conveyance or IIT crossing the border.

4.5 PROCEDURE MAINTENANCE & REVIEW

All procedures must be reviewed annually at a minimum and updated as necessary. These are to be maintained at a local operating level to be easily accessible to end users.

5.0 Conveyance & International Instruments of Traffic (IIT) Security

5.1 CONVEYANCE & IIT GENERAL

Conveyances & IIT (i.e. containers, trailers, etc.) integrity must be maintained to protect against the introduction of unauthorized material and/or persons. Inspections, both security/agricultural, and sealing procedures are a part of maintaining the ability to stuff containers on-site and remain within CTPAT compliance. Based on risk, these need to be conducted at random intervals both before and after loading.

5.2 SECURE STORAGE OF CONVEYANCE & IIT

Containers and trailers under your control or located in a facility of the under your control 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/trailers or container/trailer storage areas.



5.3 CONTAINER INSPECTIONS – 7 POINT INSPECTION FORM

Procedures must be in place to verify the physical integrity of the container structure prior to stuffing. This must be recorded on an inspection checklist, which will accompany the shipping documents. It must include an inspection and dependability assessment of the locking mechanisms on the doors. A seven-point inspection process is required for all loaded containers. A sample form for the required type of 7-point inspection process is included in [Section 15.0 Container Inspection Form](#) and [16. CBP Templates for Container Inspections](#) to assist you in planning and clearing the following inspection points. Inspections should be conducted at various locations where conveyance is susceptible to tampering or infestation.

1. Front wall
 2. Left side
 3. Right side
 4. Ceiling (inside) / Roof (outside)
 5. Floor (inside)
 6. Inside/outside doors and reliability of locking mechanisms
 7. Outside/Undercarriage
- Also, fan housing, if refrigerated container

5.4 TRACTOR & TRAILER INSPECTIONS

Procedures must be in place to verify the physical integrity of the tractor trailer structure prior to stuffing to include the reliability of the locking mechanisms of the doors. The following 17-point inspection process is recommended for all trailers [\(reference section 17. CBP Truck and Trailer inspections\)](#).

Truck	Trailers
1. Bumper/tires/rims; 2. Doors, tool compartments and locking mechanisms; 3. Battery box; 4. Air breather; 5. Fuel tanks; 6. Interior cab compartments/sleeper; and 7. Faring/roof.	1. Fifth wheel area - check natural compartment/skid plate; 2. Exterior - front/sides; 3. Rear - bumper/doors; 4. Front wall; 5. Left side; 6. Right side; 7. Floor; 8. Ceiling/roof; 9. Inside/outside doors and locking mechanisms; and 10. Outside/Undercarriage.

5.5 AGRICULTURAL INSPECTIONS

Inspections will also require an agricultural component, which has been implemented in 2020. This inspection will look for pest contamination to ensure that these foreign contaminants are not in/on the Conveyance/IIT or areas where these are stored/loaded.

Pest contamination: defined as visible forms of animals, insects or other invertebrates (alive or dead, in any lifecycle stage, including egg casings or rafts) or organic material of animal origin (including blood, bones, hair, flesh, secretions, excretions); viable or non-viable plants or plant products (including fruit, seeds, leaves, twigs, roots, bark); or other organic material, including fungi; or soil, or water; where such products are not the manifested cargo within the IIT.

Any contaminants located during the inspections should be cleaned and/or removed. Documentation to be retained for one year demonstrating compliance with the inspection requirements.



5.6 CONTAINER AND TRAILER SEAL APPLICATION

The sealing of trailers and containers, to include continuous seal integrity, are crucial elements of a secure supply chain. The party stuffing the container must immediately apply a seal that meets or exceeds the current ISO 17712 standards, with documentation, for high security seals upon stuffing. Once sealed, it should be verified following the VVTT process.

V – View seal and container locking mechanisms; ensure they are OK;

V – Verify seal number against shipment documents for accuracy;

T – Tug on seal to make sure it is affixed properly;

T – Twist and turn the bolt seal to make sure its components do not unscrew, separate from one another, or any part of the seal becomes loose.

Optionally, pictures should be taken of the container pre- and post-stuffing and of affixed seals to be forwarded to destination.

5.7 SEAL MANAGEMENT

Written procedures must stipulate how seals are inventoried, controlled and distributed prior to being affixed to loaded conveyances. These procedures must include seals being restricted to authorized personnel, secure storage, inventory, distribution, & tracking (seal log), recording the receipt of new seals, issuance of seals recorded in log, track seals via the log, and only trained, authorized personnel may affix seals to instruments of international traffic (IIT). Designated employees should be assigned to receive, distribute and maintain container seals for integrity purposes. Seal audits must be conducted periodically to ensure no seals have been removed or tampered with. Upon detection of a seal or conveyance that has been tampered with, the local GE Vernova contacts must report up through Site & Logistics escalation points.

5.8 CONVEYANCE MOVEMENT & TRACKING

When incoterms call for shipper to arrange for delivery to customer with international Customs transactions, a tracking mechanism needs to be in place for conveyance from origin to destination point. For land border shipments in proximity to the US border, a “no-stop” policy needs to be implemented regarding unscheduled stops.

6.0 Agricultural Procedures

6.1 PEST PREVENTION

Each supplier must have written procedures in place to designate the visible pest prevention measures taken, including Wood Packaging Materials (WPM) regulations, throughout the supply chain. These measures must account for the International Plant Protection Convention’s (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15, typically stamped on the wood used for crating materials). Cargo staging areas must be inspected on a regular basis to ensure the areas are visibly free of pests or infestation.

7.0 Physical Access Controls

7.1 BARRIERS TO PREVENT UNAUTHORIZED ACCESS

Physical barriers and deterrents must be in place to prevent unauthorized access to offices, trailer yards, cargo handling and storage areas. This includes manned/monitored gates where vehicles and/or personnel enter or exit. Based on risk, interior fencing should segregate high value and/or hazardous materials. This fencing/barrier should be inspected regularly to ensure integrity by designated personnel and any damages be repaired as soon as possible. Private passenger vehicles should not be allowed to park directly next to cargo areas and/or conveyances.



7.2 SECURITY TECHNOLOGY & MONITORING

Licensed/certified resources should be considered when designing and installing security technology. Areas inside and outside the facility including cargo handling, storage, and parking areas must have adequate lighting. Alarms should be used to detect unauthorized access to any sensitive areas. A policy with procedures must be in place for any equipment used to monitor or detect a breach or risk whereby it is regularly reviewed for placement/positioning, performance, maintenance, and physically secured from unauthorized access to said equipment. The results of monitoring/testing/recording reviews should be documented and any corrective actions that apply for audit purposes. This policy must be reviewed annually dependent upon risk. If a camera system is used, it must have one positioned on key areas of the facility that are tied to the import/export process. Random reviews should be conducted by management/security to verify cargo security procedures are being followed in accordance with law. Findings must have corrective actions assigned and records maintained for audit. Security systems and technology should have a backup power source and report failure to record. Cameras should be set to record at the highest and most reasonable quality setting with 24/7 recording. Recordings should be maintained for a sufficient amount of time as they pertain to potential investigations.

8.0 Access Controls

8.1 EMPLOYEE BADGING, PERSONNEL IDENTIFICATION, & ACCESS CONTROL

An employee identification system must be in place for positive identification purposes. Written procedures for badging & access devices must be in place to determine when access is granted, changed, or removed. Company management or security personnel must adequately control the issuance and removal of employee, visitor and vendor identification badges. Sensitive areas must have controls for access based on criteria such as job description, duty, etc. Access must be removed upon employee separation from the company.

8.2 VISITORS, VENDORS, & SERVICE PROVIDER ACCESS CONTROL

Visitors, vendors, and service providers a photo identification must be provided upon arrival using a log that is maintained with reasons and details of the visit. Visitor vehicles may be subject to search in accordance with local and labor laws. Visitors should be escorted while on premises. The following information must be included on the visitor's log: date of visit, visitor's name, verification of photo identification (type verified: license, national ID card, etc.), time of arrival, company point of contact, and time of departure. Access to sensitive areas must not be provided beyond scope of visit. Issued badging must always be visibly displayed during visit.

8.3 DRIVERS & CARGO LOGGING

Drivers delivering or receiving cargo must be positively identified before cargo is received or released. Drivers must present an acceptable photo identification (government or employer issued ID) to the facility employee granting entrance. A cargo pickup log must be kept registering the record of the driver/conveyance when picking up cargo. This log must be kept in a secure place away from drivers or others who might tamper with it. Cargo log should include the following: driver's name, date, time of arrival, employer, truck number, trailer number, time of departure, and the seal number affixed to the shipment at the time of departure. Where operationally feasible, pickups and deliveries should be by appointment only, with carrier notifying location of planned arrival time, driver name, and truck number. Inbound packages/mail should be periodically screened before being admitted.

8.4 SECURITY POLICIES & SECURITY GUARDS

If security guards are used, work instructions must be in place with policies/procedures for the tasks they are to perform on your behalf. These policies and those mentioned above must be reviewed and updated periodically by the management of the group to ensure compliance and appropriateness. Annual audits should be conducted of these practices to ensure compliance, or as threat/risk level dictates.



9.0 Training

9.1 EMPLOYEE/CONTRACTOR EDUCATION & TRAINING

Security training for involved employees & contractors is imperative for an effective CTPAT member. There must be a program in place that promotes awareness of security risks and measures to be taken to adhere to requirements (by job). CTPAT training should be provided to new employees as they are onboarded to pair with annual trainings. Training must include reporting security incidents and suspicious activities. Trainings need to be tracked including date of the trainings, sign in sheets, name of the attendees, and topics of the training. This requirement applies to periodic refresher training as well. The training measures should be verifiable to ensure objectives were met. Drivers and other security personnel must be trained to find hidden compartments and pest contaminations. All employees are required to know how to report security incidents and suspicious activities. As applicable, employees need to be trained in the company's cybersecurity policies and security equipment (when operating), including protecting electronic information/data.

10.0 Cyber Security

10.1 POLICIES & PROCEDURES

Comprehensive written cybersecurity policies/procedures must be in place to protect information technology (IT) systems. These policies must cover individual cybersecurity, data breach, social engineering, personal device usage, and should be reviewed annually. Procedures must include recovery or replacement of IT systems and/or data. Policies should address how information is shared around cybersecurity threats with the government and other business partners. Measures to prevent the use of counterfeit or improperly licensed technological products should be in place. If there is use of employee owned devices, these must adhere to the company's cybersecurity policy. Cybersecurity policy violators must be subject to appropriate disciplinary actions. Reference [GE Vernova Third Party Information Security Requirements](#) for additional requirements that may apply.

10.2 PROTECTIVE MEASURES

A system is required to be in place to prevent unauthorized access of IT systems/data, abuse of policies including improper access of internal systems or external websites, and tampering/altering business data by employees/contractors. Security software must receive regular updates. Network systems must be tested regularly for vulnerabilities with corrections as soon as feasible upon detection. Security software used must receive regular updates. Data should be appropriately backed up, with sensitive data being encrypted. Users of IT systems must have individual accounts assigned. Strong passwords must be used for authentication. User access must be restricted based on job description or assigned duties. Access must be reviewed on a regular basis to ensure that it is available only to those who require it, specifically sensitive systems. Computer and network access must be removed upon employee separation. Users who remotely access the network must be connected through VPN or have multi-factor authentication to ensure network security integrity.

10.3 HARDWARE MANAGEMENT

All media, hardware, and other IT equipment (containing sensitive information regarding import/export process) must be accounted for through regular inventories. When disposed, items must be sanitized and/or destroyed in accordance with the National Institute of Standards & Technology (NIST) Guidelines for Media Sanitization or other industry guideline.



11.0 Personnel Security

11.1 PERSONNEL SECURITY OVERVIEW

Implementing personnel security measures is an important step in securing the supply chain. The focus of a written personnel security program is to investigate the background of prospective employees to ensure that they pose no risk to a company's operations. Please note that the requirements provided below are based on U.S. standards and may not be possible to fulfill in other countries. However, GE Vernova expects all suppliers to take as many steps as possible to avoid hiring someone that may pose a threat to the company or its supply chain. An employee code of conduct must also be in place to define expectations and acceptable behaviors.

11.2 PRE-EMPLOYMENT VERIFICATION

Prospective employees must undergo pre-screening background checks prior to commencement of employment. This applies to prospective permanent, temporary, and contract employees. Application information, such as employment history and references must be verified prior to employment.

11.3 CONTINUED-EMPLOYMENT VERIFICATION

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

11.4 BACKGROUND CHECKS / INVESTIGATIONS

Background checks should include the following:

- All felony and misdemeanor convictions involving workplace violence, burglary/robbery, theft, assault, identity theft, murder, rape, terrorist threats, or other crimes.
- Application verification
- Prior employment
- Address verification
- Photographs of all employees should be kept on file

11.5 PERSONNEL TERMINATION PROCEDURES

GE Vernova expects all service providers to have procedures in place to remove identification, facility and system access for terminated employees.



12.0 Material Supplier Acknowledgement for Security Program

Participants

Company Name	_____	Date	_____
Company Address	_____ _____ _____		
Respondent Name	_____	Phone	_____
Title	_____	Email	_____
Certification Status	C-TPAT Validated	Date of latest revalidation	_____
Company Certified Name	_____	SVI#	_____
Signature	_____		

I, _____ a duly authorized representative of the above-mentioned company, do hereby acknowledge and confirm the following.

- ☐ I have received and reviewed a copy of GE Vernova Gas Power's C-TPAT Expectations for Material Suppliers.
- ☐ I clearly understand my Company's responsibilities as a Material Supplier is ensuring the security and integrity of the Supply Chain.
- ☐ I attest that my Company can meet and/or exceed all C-TPAT Supply Chain Expectations for Material Suppliers.
- ☐ I understand that GE Vernova can/will hold my company liable for C-TPAT security compliance of all subcontractors used by my company in the transportation of its merchandise within the supply chain.
- ☐ I understand that GE Vernova reserves the right to provide recommendations for the improvement of my Company's Supply Chain Security.
- ☐ I understand that GE Vernova or their contracted service provider and/or U.S. Customs reserves the right to physically inspect my company's facilities.
- ☐ I understand that GE Vernova reserves the right to cease doing business with my company should our C-TPAT status change.

MRA Program Participation	Name of Program	Date of Certification
Certification Identifier Number	_____	_____
Signature		



13.0 Material Supplier Acknowledgement Form – Other

Company Name	_____	Date	_____
Company Address	_____ _____		
Respondent Name	_____	Phone	_____
Title	_____	Email	_____

I, _____ a duly authorized representative of the above-mentioned company, do hereby acknowledge and confirm the following.

- ☐ I have received and reviewed a copy of GE Vernova Gas Power's C-TPAT Expectations for Material Suppliers.
- ☐ I clearly understand my Company's responsibilities as a Material Supplier is ensuring the security and integrity of the Supply Chain.
- ☐ I attest that my Company can meet and/or exceed all C-TPAT Supply Chain Expectations for Material Suppliers.
- ☐ I understand that GE Vernova can/will hold my company liable for C-TPAT security compliance of all subcontractors used by my company in the transportation of its merchandise within the supply chain.
- ☐ I understand that GE Vernova reserves the right to provide recommendations for the improvement of my Company's Supply Chain Security.
- ☐ I understand that GE Vernova or their contracted service provider and/or U.S. Customs reserves the right to physically inspect my company's facilities.
- ☐ I understand that GE Vernova reserves the right to cease doing business with my company should our C-TPAT status change.

Authorized Logistics Service Providers Signature

Date

Company Stamp/Seal



14.0 Status of Mutually Recognized Arrangements (MRAs)

As of September 2018, CBP has signed eleven MRAs:

- New Zealand - June 2007 – [New Zealand Customs Service's Secure Export Scheme Program](#)
- Canada - June 2008 – [Canada Border Services Agency's Providers in Protection Program](#)
- Jordan - June 2008 – [Jordan Customs Department's Golden List Program](#)
- Japan - June 2009 – [Japan Customs and Tariff Bureau's Authorized Economic Operator Program](#)
- Korea - June 2010 – [Korean Customs Service's Authorized Economic Operator Program](#)
- European Union - May 2012 – [European Union's Authorized Economic Operator Program](#)
- Taiwan - November 2012– [Directorate General of Customs, Taiwan Ministry of Finance's – Authorized Economic Operator Program*](#)
- Israel – June 2014 - [Israel Tax Authority's Authorized Economic Operator Program.](#)
- Mexico - October 2014 - [Mexico OEA Certification \(Authorized Economic Operators\) formerly known as NEEC.](#)
- Singapore – December 2014 – [Singapore Customs' Secure Trade Providership \(STP\) Program](#)
- Dominican Republic - December 2015 – [Authorized Economic Operator Program – AEO](#)
- Peru – September 2018 – Authorized Economic Operator Program - AEO

**Note: This MRA is signed between the American Institute in Taiwan (AIT) and the Taipei Economic and Cultural Representative Office (TECRO) in the United States. CTPAT and Taiwan AEO are the designated parties responsible for implementing the MRA.*

For the latest published MRAs, visit: <https://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism/mutual-recognition>

15.0 Container Inspection Form

Date _____

Container # _____ Seal # _____ Total Cartons _____

Shipper/Vendor _____ Consigned to _____

Transported by: _____ Supervisor Initials: _____
(As needed)

Container Inspection Record			
Inspection	Check if Acceptable	Describe noted condition (If there is a noted change condition or manifested material, please describe here – a supervisor must verify, confirm and initial any form that has conditions noted.)	
Outside/Undercarriage	<input type="checkbox"/>		
Right Side	<input type="checkbox"/>		
Left Side	<input type="checkbox"/>		
Ceiling/Roof	<input type="checkbox"/>		
Front Wall	<input type="checkbox"/>		
Inside/Outside	<input type="checkbox"/>		
Floor	<input type="checkbox"/>		
Seal Verification	<input type="checkbox"/>		
<input type="checkbox"/> I have visually inspected and verified, to the best of my ability, the condition of the container noted above. I confirm that the container appears structurally sound, weather tight, has no false compartments, contains no manifested material, and the locking mechanisms are in good order showing no visible signs of tampering.			
<input type="checkbox"/> I have noted the condition found and advised by supervisor – the container is NOT approved as is.			
Inspected by:		Date:	
Seal Affixed and verified by:		Time:	

1 - COPY of completed form should be included with paperwork presented with the cargo to approved Freight Forwarder or Customs Broker

2- COPY retained with file – and submitted with information for payment

16.0 CBP Created Templates for Container Inspections



Printed name of person who conducted security inspection upon arrival: _____ Signature: _____

Inspection was completed: Date: _____ Time: _____

Printed name of person who conducted follow up security inspection: _____ Signature: _____

Seal number(s) that was on container when it arrived at this facility: _____

Seal number(s) that was on container when it departed this facility: _____

Printed name of person who affixed seal(s): _____ Signature: _____

Printed name of person who verified physical integrity of seal(s): _____ Signature: _____

17.0 CBP created templates for Truck and Trailer inspection

This inspection must be completed and documented on all containers/trailers/conveyances bound for the USA.

17-Point Truck & Trailer Inspection

17
Point



Strengthening the Customs-Trade Cooperative Partnership



Printed name of person who conducted security inspection upon arrival: _____ Signature: _____
Inspection was completed: Date: _____ Time: _____
Printed name of person who conducted follow up security inspection: _____ Signature: _____
Seal number(s) that was on container when it arrived at this facility: _____
Seal number(s) that was on container when it departed this facility: _____
Printed name of person who affixed seal(s): _____ Signature: _____
Printed name of person who verified physical integrity of seal(s): _____ Signature: _____