C-TPAT SECURITY ASSESSMENT

C-TPAT Security Assessment

C-TPAT. (Customs-trade Partnership Against Terrorism) is a voluntary government business initiative designed to build cooperative relationships that strengthen and improve overall international supply chain and U.S. border security. Through this initiative, U/S/ Customs and Border Protection (CBP) is asking business to ensure the integrity of their security practices and communicate and verify the security guidelines of their business partners within the supply chain.

As a certified and validated member of C-TPAT, JSI Logistics must assess the security practices of our customers and service providers. This Supply Chain Security Questionnaire serves as a tool for that assessment.

Please complete the attached questionnaire to the best of your ability (electronically or in hard copy and return it within ten days of receipt to:

Yvonne Fazzino
JSI Logistics
1535-B Rollins Road
Burlingame, CA 94010
Phone Number: 650-697-3963 x1458
Fax Number: 650-697-3831
YFazzino@jsilogistics.com

NOTE: If your company has already received C-TPAT certification, completion of only the first page of the questionnaire is necessary.

Thank you in advance for your time and cooperation.

Customer/Supplier Information	
Company Name	
Type of Business	
Address	
City, State, ZIP	
Respondent's Name	
Respondent's Title	
Telephone	
Fax	
Email	
Date of Completion	

Indicate C-TPAT Status

Check Appropriate Box:

- ❑ **Certified
- ❑ Pending Application
- ❑ Not Applicable

_____

**SVI No.

**Certified C-TPAT Participants: Please provide your SVI number. Completion of the questionnaire is optional.

C-TPAT SECURITY ASSESSMENT

A. Security Management System	Yes	No	Notes/Additional Information
1. Is there a manager responsible for implementing security within the company? Please provide name and contact information.			
2. Do written security policies and procedures exist?			
3. Is there a documented process for reporting and investigating security related incidents?			
4. Are periodic security audits/reviews conducted?			

B. Physical Security	Yes	No	Notes/Additional Information
1. Do written Physical Security standards exist?			
2. Are company premises protected from unauthorized access by perimeter fencing or natural barriers?			
3. Are controls in place to prevent unauthorized vehicles from entering company premises?			
4. Are private passenger vehicles prohibited from parking in or adjacent to cargo handling and storage areas, aircraft, and trucks?			
5. Are all company buildings constructed of materials that resist unlawful entry and protect against outside intrusion?			
6. Is driver/customer access to the interior of Company facility limited to a secure, segregated waiting area?			
7. Are procedures in place to identify, challenge and address unauthorized/ unidentified persons?			
8. Are employees and authorized visitors positively identified with photo identification or other means?			
9. Are visitors/contractors logged in, badged, and escorted?			

B. Physical Security cont.	Yes	No	Notes/Additional Information
10. Is adequate lighting provided inside and outside company facility to include parking areas?			
11. Are all doors/windows/openings locked to prevent unauthorized access to the facility and are they monitored by an intrusion detection/burglar alarm system?			
12. Is there a working CCTV (Closed Circuit Television) system that covers monitors and records:			
a. Exterior of buildings?			
b. Personnel entrances?			
c. Interior and exterior of the docks, and yards where trailers and containers are loaded/unloaded or stored?			

C. Human Resources (Personnel Security, Training & Awareness)	Yes	No	Notes/Additional Information
1. Are pre-employed background checks conducted that includes criminal checks and application verification to the fullest extent allowed by law?			
2. Are periodic background checks conducted for current employees?			
3. Is there a process for handling terminated employees or contracted and preventing subsequent access to the premises?			
4. Do you have a documented company Code of Conduct?			
5. Do all employees receive security and threat awareness training?			

D. Conveyance Integrity (Aircraft, Vessel, Container, Trailer/Truck)	Yes	No	Notes/Additional Information
1. Are there written security procedures covering receipt, loading and unloading of containers/trucks to prevent cargo loss or the introduction of unauthorized or unmanifested material?			
2. Is conveyance integrity maintained to prevent the introduction of unauthorized personnel or material into aircraft/vessel/container/trucks?			
3. Do these procedures ensure the timely reporting to law enforcement?			
4. Are procedures in place to ensure unauthorized and unidentified persons are challenged and prevented access to the premises, yards, and conveyances?			
5. Are all trucks/containers sealed and or locked to prevent the introduction of unauthorized personnel or unmanifested cargo?			
6. Are “High Security” seals used? (Provide certification details)			
7. Are Seals kept under lock and key to prevent unauthorized access and misuse?			
8. Are all conveyances inspected upon arrival or at transfer points for signs of tampering?			
9. Is there a system evident to monitor and track the timely movement of all cargo conveyances?			
10. Is vehicle/conveyance tracking, tracing and intrusion detection available in real time? Describe.			
11. Does your company perform the recommended container “7 point inspection”?			

E. Information Technology (IT) Security	Yes	No	Notes/Additional Information
1. Are systems accessed with user accounts and passwords?			
2. Is a system in place to identify abuse of IT systems including improper access, tampering or the altering of business data?			
3. Are IT security policies, procedures and standards in place and provided to employees through training?			
4. Is there a system in place to ensure the removal of system access for terminating employees?			

F. Business Partner Selection (Vendor/Service Provider/Agent)	Yes	No	Notes/Additional Information
1. Does the company have written and verifiable processes for the screening and selection of business partners?			
2. Do you consider security capabilities and practices in your vendor selection process?			
3. Are all selected and potential business partners notified by the company that they must become compliant with C-TPAT equivalent guidelines in order to conduct business with the company?			
4. Do your contracts with service providers specify the minimum security requirements expected of them?			

G. Shipping and Receiving Procedures (Manifest Procedures)	Yes	No	Notes/Additional Information
1. Are procedures in place at shipping and receiving locations to ensure that shipping documents are complete, legible and accurate?			
2. Are procedures available, evident, and adequate to ensure cargo is properly marked and manifested to include accurate weight and piece count?			

H. Other Security Measures

Please use the space below to describe vulnerabilities or additional security measures you have to plan to put in place that were not previously covered.

Additional information on the C-TPAT program is available on the web at: http://www.cbp.gov/ctpat