

ISUZU CUSTOMS OPERATIONS

North American Free Trade Agreement (NAFTA)

This section applies to suppliers of parts and components that originate in Canada or Mexico and are shipped directly to Isuzu or a facility designated by Isuzu.

NAFTA Certificate - General Requirements for Supplier

- A copy of the NAFTA Certificate of Origin (NAFTA Certificate) for each NAFTA qualified part should be issued to the INAC Purchasing Department prior to the first shipment of that part for each calendar year.
- If a copy of the NAFTA Certificate will not be available prior to the first shipment to Isuzu for each calendar year, the INAC Purchasing Department must be immediately notified.
- The preferred method to receive the NAFTA Certificate is as an e-mail attachment. If unable to email with signature please fax.
- NAFTA Certificates must only be issued to the INAC Purchasing Department. Under no circumstances should the NAFTA Certificate be issued directly to the motor carrier, customs broker or any other party without the consent of the INAC Purchasing Department.
- The full 10 digit Isuzu part number must be shown on the NAFTA Certificate.
- Each NAFTA Certificate must be clearly legible, signed, and dated.
- The NAFTA Certificate must show the correct Isuzu company as importer. It is acceptable to show "various" in the importer box on the NAFTA Certificate if the part(s) will be imported by more than one Isuzu company.

NAFTA Certificate - H.S. Tariff Classification

- For new Isuzu parts, the determination of the correct H.S. tariff classification should be coordinated with the Isuzu Customs Department through the INAC Purchasing Department.
- For existing Isuzu parts in which the classification shown on the NAFTA Certificate doesn't match the classification in the Isuzu classification database, the Isuzu Customs Department will submit a classification change request to the INAC Purchasing Department. The INAC Purchasing Department will coordinate with the supplier to revise the NAFTA Certificate.

Free Trade Agreements General Provisions

NAFTA, Chile Free Trade, Singapore Free Trade, and any future enacted Free Trade Agreement Certificates should be issued to the INAC Purchasing Department, in a timely manner each year, for "all" parts supplied to Isuzu. This enables Isuzu to comply with vehicle content origin and export regulations.

Customs - Trade Partnership Against Terrorism (C-TPAT)

This section applies to all foreign suppliers. For the purposes of this manual, a foreign supplier is defined as any person, business or corporation that provides, sells, ships or distributes, directly to Isuzu, any product originating from outside the U.S. and U.S. Territories. Isuzu encourages all eligible foreign suppliers to become certified C-TPAT members.

Each foreign supplier:

- Must review the “Isuzu C-TPAT Expectations for Supplier” handbook (see *Appendix A*). Isuzu strongly encourages each foreign supplier to comply with the security criteria and guidelines contained in the “Isuzu C-TPAT Expectations for Supplier” handbook.
- Should develop security processes and procedures consistent with the C-TPAT security criteria contained in the “Isuzu C-TPAT Expectations for Supplier” handbook.
- Must complete the Isuzu “Security Self-Assessment for Suppliers” questionnaire (see *Appendix B*). The completed questionnaire must be returned to the Isuzu Purchasing Dept. and updated as necessary.
- Must allow Isuzu to conduct periodic reviews and verification of foreign suppliers’ processes and facilities as it relates to C-TPAT security criteria.
- Should indicate to the Isuzu Purchasing Dept., and update as required, their status of participation in obtaining certification in a supply chain security program administered by a foreign Customs Administration.
- Complying with or meeting the C-TPAT security criteria as set forth in the “Isuzu C-TPAT Expectations for Supplier” handbook must submit a letter to Isuzu from a senior officer attesting to such compliance.

Country of Origin Marking

This section applies to all foreign suppliers. Unless accepted by law, all parts and components (or its container) of foreign origin must be properly marked with the name of the country of origin. If there are any questions regarding specific requirements of this section, please contact the INAC Customs Operations Dept. through the INAC Purchasing Dept.

Wood Packaging Material (WPM)

This section applies to all foreign suppliers. The U.S. has adopted the international standard for wood packaging material (WPM) used in international commerce that was approved by the International Plant Protection Convention (IPPC). Subject WPM include most pallets, crates, dunnage and blocking and bracing materials. The international standard requires affected WPM to be either heat-treated or fumigated in accordance to the established guidelines and marked with an approved international mark certifying such treatment. Import

shipments found to contain non-compliant WPM will not be allowed entry into the U.S. Isuzu requires all subjected WPM to be properly treated and marked.

CUSTOMS FORMS & APPENDIXS

1. NAFTA Certificate (sample)
2. UCFTA Certificate (sample)
3. Appendix A C-TPAT Expectations
4. Appendix B Self-Assessment Form

**DEPARTMENT OF THE TREASURY
UNITED STATES CUSTOMS SERVICE
NORTH AMERICAN FREE TRADE AGREEMENT
CERTIFICATE OF ORIGIN
(INSTRUCTIONS ATTACHED)
19 CFR 181.11, 181.22**

Approved through 12/31/96.
OMB No. 1515-0204.
See back of form for Paper-
work Reduction Act Notice.

1. EXPORTER/SUPPLIER NAME AND ADDRESS: TAX ID NUMBER:	2. BLANKET PERIOD:(DD/MM/YY) FROM: TO:					
3. PRODUCER NAME AND ADDRESS: TAX ID NUMBER:	4. IMPORTER NAME AND ADDRESS: TAX ID NUMBER:					
5 DESCRIPTION OF GOODS	6 H.S. TARIFF CLASS #	7 PREFERENCE CRITERION	8 PRODUCTION COUNTRY	9 NET OF	10 COUNTRY OF ORIGIN	11 TRACED VALUE
<div style="font-size: 4em; color: red; opacity: 0.5; transform: rotate(-45deg); pointer-events: none;"> SAMPLE </div>						
I CERTIFY THAT: -THE INFORMATION ON THIS DOCUMENT IS TRUE AND ACCURATE AND I ASSUME THE RESPONSIBILITY FOR PROVING SUCH REPRESENTATIONS. I UNDERSTAND THAT I AM LIABLE FOR ANY FALSE STATEMENTS OR MATERIAL OMISSIONS MADE ON OR IN CONNECTION WITH THIS DOCUMENT. -I AGREE TO MAINTAIN AND PRESENT UPON REQUEST, DOCUMENTATION NECESSARY TO SUPPORT THIS CERTIFICATE, AND TO INFORM, IN WRITING, ALL PERSONS TO WHOM THIS CERTIFICATE WAS GIVEN OF ANY CHANGES THAT COULD AFFECT THE ACCURACY OR VALIDITY OF THIS CERTIFICATE. -THE GOODS ORIGINATED IN THE TERRITORY OF ONE OR MORE OF THE PARTIES, AND COMPLY WITH THE ORIGIN REQUIREMENTS SPECIFIED FOR THESE GOODS IN THE NORTH AMERICAN FREE TRADE AGREEMENT, AND UNLESS SPECIFICALLY EXEMPTED IN ARTICLE 411 OR ANNEX 401, THERE HAS BEEN NO FURTHER PRODUCTION OR ANY OTHER OPERATION OUTSIDE THE TERRITORIES OF THE PARTIES; AND -THIS CERTIFICATE CONSISTS OF <u> 1 </u> PAGES, INCLUDING ALL ATTACHMENTS.						
12A. AUTHORIZED SIGNATURE:			12B. COMPANY:			
12C. NAME (PRINT OR TYPE):			12D. TITLE			
12E. DATE: (DD/MM/YY)		12F. TELEPHONE:		FAX:		

**UNITED STATES - CHILE FREE TRADE AGREEMENT
 TRATADO DE LIBRE COMERCIO CHILE – ESTADOS UNIDOS
 CERTIFICATE OF ORIGIN**

Field 1: Exporter Name and Address Field 1a: Supplier Name and Address Duns Number: Tax Identification Number:		Field 2: Blanket Period for Multiple Entries From: To:				
Field 3: Producer Name and Address Tax Identification Number:		Field 4: Importer Name and Address Tax Identification Number:				
Field 5: Description of Good(s)	Field 6: HS Tariff Classification Number	Field 7: Preference Criterion	Field 8: Producer	Field 9: Regional Value Content	Field 10: Country of Origin	
<div style="font-size: 4em; color: red; opacity: 0.5; transform: rotate(-30deg); pointer-events: none;"> SAMPLE </div>						
Field 11: Certification of Origin I CERTIFY THAT: <ul style="list-style-type: none"> THE INFORMATION ON THIS DOCUMENT IS TRUE AND ACCURATE AND I ASSUME THE RESPONSIBILITY FOR PROVING SUCH REPRESENTATIONS. I UNDERSTAND THAT I AM LIABLE FOR ANY FALSE STATEMENTS OR MATERIAL OMISSIONS MADE ON OR IN CONNECTION WITH THIS DOCUMENT. I AGREE TO MAINTAIN, AND PRESENT UPON REQUEST, DOCUMENTATION NECESSARY TO SUPPORT THIS CERTIFICATE, AND TO INFORM, IN WRITING, ALL PERSONS TO WHOM THE CERTIFICATE WAS GIVEN OF ANY CHANGES THAT COULD AFFECT THE ACCURACY OR VALIDITY OF THIS CERTIFICATE. THE GOODS ORIGINATED IN THE TERRITORY OF THE PARTIES, AND COMPLY WITH THE ORIGIN REQUIREMENTS SPECIFIED FOR THOSE GOODS IN THE UNITED STATES-CHILE FREE TRADE AGREEMENT, AND UNLESS SPECIFICALLY EXEMPTED IN ARTICLE 4.11, THERE HAS BEEN NO FURTHER PRODUCTION OR ANY OTHER OPERATION OUTSIDE THE TERRITORIES OF THE PARTIES. 						
Authorized Signature		Company Name				
Name (Print or Type)		Title				
Date (MM/DD/YY)		Telephone / Fax				
Field 12: Remarks						

*C-TPAT Expectations for
Foreign Suppliers*

ISUZU

March 2016

Table of Contents

Introduction	3
1. Procedural Security	4
2. Physical Security	5
3. Access Controls	7
4. Personnel Security	8
5. Education & Awareness Training	9

Isuzu North America Corporation
Isuzu Motors America, LLC
Isuzu Commercial Truck of America, Inc.
Isuzu Technical Center America, Inc.
(Collectively Isuzu)

C-TPAT Expectations for Suppliers

Background

In the wake of 9/11 U.S. Customs and Border Protection (CBP) immediately tightened security at U.S. borders and cautioned the importing community of the susceptibility of the supply chain to breaches in cargo security. It also prompted CBP to institute a voluntary security program known as the Customs Trade Partnership Against Terrorism (C-TPAT). This joint initiative between CBP and the global business community has not only made the supply chain more secure but it has provided visible benefits to those companies that have joined. In exchange for implementing improved security practices and communicating security requirements to their business partners, importers have experienced reduced inspections and quicker clearance of imported freight. By participating in the C-TPAT program, ISUZU hopes to increase vigilance amongst its employees and partners and establish a more secure & efficient supply chain.

We understand that if our supply chain was disturbed by an act of terror, it could have a significant impact on our business and business relationships. Therefore, we are asking the vendors we do business with to enhance their safety and security procedures in the following areas: procedural security, physical security, conveyance security, access controls, personnel security, and education & awareness training.

ISUZU has developed a list of requirements for each of these specific areas of focus. We recognize that some of the requirements may be 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 vendors due to the size of their factory and structure. However, it is important for each manufacturer to acknowledge that security regulations are formulated and implemented to protect both the company and its employees. It is imperative that all employees observe the facility security policies and report any suspicious or improper actions to management and/or the proper authorities.

ISUZU reserves the right to conduct background investigations on manufacturers before doing business with them. In particular, ISUZU is interested in investigating the company for financial solvency, and the principles for criminal activity.

1. Procedural Security

Procedural Security measures regulate incoming and outgoing goods and are designed to prevent the introduction of unmanifested materials into the supply chain, or the loss or exchange of ISUZU merchandise.

- 1.1 Each factory should have a designated employee supervising the introduction and removal of cargo.
- 1.2 All merchandise must be properly marked, weighed, counted, and documented.
- 1.3 Procedures must be in place to govern the detection and recording of shortages and overages.
- 1.4 Containers, trailers, and/or railcars left at the facility overnight must be secured. Containers that are full of cargo must be locked and sealed with industry-approved seals and corresponding seal numbers must be recorded. The seals must be uniquely numbered and require destruction to be removed.
- 1.5 The factory should have a procedure for inspecting and verifying seals. Discrepancies must immediately be reported to management and/or security personnel.
- 1.6 All containers or trailers entering or leaving the facility must be recorded, along with the name of the driver who took custody of the merchandise.
- 1.7 All security procedures must be documented with formal self-assessments (see attached) completed every year. Copies of the self-assessment must be forwarded to ISUZU's Purchasing Manager.
- 1.8 ISUZU conducts assessments on a periodic basis. ISUZU or its agents shall have the right to conduct assessments at all reasonable times upon prior notice to supplier.

2. Physical Security

Factories from which ISUZU sources merchandise should have the following characteristics:

- 2.1 Buildings must be constructed of materials that resist unlawful entry and protect against outside intrusion.
- 2.2 Entrances & exits must be monitored. Doors should be locked or otherwise secured when not in use.
- 2.3 External and internal doors, windows, and fences must be protected by appropriate means.
- 2.4 Alarms installed to detect unauthorized entry after hours. Systems should be monitored by a security guard or outside security agency.
- 2.5 External doors are alarmed and linked to the main alarm system.
- 2.6 Windows are secured with alarms or other protective barriers/deterrents (bars, etc.).
- 2.7 Reinforced exit doors. Likewise, dock doors should be constructed of materials that prevent unlawful entry.
- 2.8 Adequate lighting inside and outside the facility. All corners of parking lots should be illuminated at night. Inside lighting should be bright enough to eliminate dark spots or corners.
- 2.9 Flood lighting on loading and unloading areas. Dock doors should be illuminated at night.
- 2.10 Clear zones must be maintained internally and externally to monitor the security of the facility. Brush and other growth should be cleared at least 35 feet from perimeter barrier.
- 2.11 A guard or receptionist to monitor office entrances.
- 2.12 There must be a formal registration process for documenting visitors to the operations.
- 2.13 Parking for employees must be separate from the dock and cargo operations.
- 2.14 All containers and trailers that remain at the warehouse overnight should be secured. Trailers loaded with cargo should also be sealed, with the seal number recorded and verified.

- 2.15 Container and trailer seal numbers must be verified before the trailer or truck is released.
- 2.16 Employees should be familiar with the trucking vendors. The identification of the driver should be checked before cargo is released to his or her custody.
- 2.17 Truck drivers should never be allowed to randomly enter the factory and pick up a trailer without supervision.
- 2.18 Each facility should also have communication systems in place to contact internal security personnel or local law enforcement in the event of an emergency.

3. Access Controls

Factories from which ISUZU sources merchandise are expected to meet the requirements detailed below. We understand that all measures may not be appropriate for all factories because of differences in size, operation and structure. However, the vendor should strive to implement as many measures as necessary to ensure that access to ISUZU merchandise is restricted to authorized employees.

- 3.1 Factories should have a formal system for identifying both permanent and temporary employees. Ideally, ID badges with the employee's name and picture should be used.
- 3.2 Badges should be visible at all times. Employees must be required to show their badge upon entering the facility.
- 3.3 Badges should be color-coded to help distinguish workers from assigned areas to various areas of the operation.
- 3.4 Factories should limit employee access to loading docks. Only employees scheduled to work on the loading docks or otherwise approved should be granted access.
- 3.5 All facilities must have a controlled access gate that monitors activity coming in and out of the facility. All containers, trailers, drivers must be logged in and out of the facility.
- 3.6 Visitors should be formally registered and must be required to wear a visitor badge at all times.
- 3.7 An employee must escort all visitors while in a loading facility or warehouse.
- 3.8 Employees or security personnel must challenge unknown persons in the facility.
- 3.9 Computers or networks containing sensitive trade data should be secured so as to prevent unauthorized access to such data. Computer workstations and the network should be password-protected.
- 3.10 Any information in the public domain (e.g., the Internet) must be protected by a firewall.
- 3.11 Limited access should be granted to sensitive information; employees should only have access to information that directly pertains to their job. A log of access rights should be maintained. Once employees are terminated, access rights must be revoked.

4. Personnel Security

Implementing personnel security measures is an important step in securing the supply chain. The focus of a personnel security program is to investigate the background of prospective employees to ensure that they pose no risk to ISUZU'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, we expect all manufacturers we do business with to take as many steps as possible to avoid hiring someone whom may pose a threat to ISUZU or its supply chain.

- 4.1 Prospective employees must undergo pre-screening prior to commencement of employment. This applies to prospective permanent, temporary, and contract employees. Manufacturers should conduct a background check of all prospective employees.
- 4.2 The background check should include the following:
 - 4.2.1 Criminal convictions – All felony and misdemeanor convictions involving workplace violence, burglary/robbery, theft, assault, identity theft, murder, kidnapping, rape, terrorist threats, or other crimes.
 - 4.2.2 Application verification
 - 4.2.3 Prior employment
 - 4.2.4 Address verification
- 4.3 Photographs of all employees should be held on file.

5. Education and Training Awareness

- 5.1 To promote security in the supply chain, our vendors should develop a formal security training program for all employees.
- 5.2 The training program should address the following:
 - 5.2.1 Recognizing internal conspiracies
 - 5.2.2 Maintaining product integrity
 - 5.2.3 Discovering and addressing unauthorized access of the facility or information
- 5.3 Employees should receive security training within the first 30 days of being hired, and all training should be documented and available for review.
- 5.4 The training program should be included in the factory's self-audit process.
- 5.5 Incentives should be established to encourage employees to actively participate in security programs and communicate potential security issues involving theft, conspiracy, or terrorist activities.
- 5.6 ISUZU reserves the right to approve vendors' education & training programs. ISUZU further reserves the right to conduct yearly audits of the programs.

*Security Self –Assessment
For Suppliers*



ISUZU

Isuzu North America Corporation
 Isuzu Motors America, LLC
 Isuzu Commercial Truck of America, Inc.
 Isuzu Technical Center America, Inc.
 (Collectively Isuzu)

Security Self-Assessment for Suppliers

Facility Under Review:	Date:
Respondent Name:	Respondent Title:

NOTE: Some questions may not apply in whole or in part to your facility. In these cases, please do not leave the question blank. Instead, state "not applicable" ("N/A") in the "Brief Description of Procedure" field and provide an explanation for your reasoning.

1. Procedural Security

1. Procedural Security			
Question	Yes	No	Brief Description of Procedure
1.1 Does your facility have a formal security department or a designated security officer to supervise the introduction and removal of cargo and packages?			
1.2 Do you verify the cargo against the manifest documents?			
1.3 How do you detect and account for overages or shortages?			
1.4 If containers or trailers are left at the facility overnight, are they secured, locked, and sealed as necessary? If the containers/trailers are full of cargo, are they also sealed?			
1.5 Is a procedure in place for inspecting and verifying seals, and for immediately reporting discrepancies?			
1.6 Are containers, trailers, and drivers that enter or leave the facility recorded?			
1.7 Are security procedures documented?			
1.8 Do you conduct formal self-assessments of security procedures?			

2. Physical Security

Question	Yes	No	Brief Description of Procedure
2.1 Are buildings constructed of materials that resist unlawful entry and protect from outside intrusion?			
2.2 Are entrances and exits monitored? Are they locked and secured when not manned?			
2.3 Are external and internal doors, windows, and/or fences protected from outside intrusion?			
2.4 Are intrusion alarms used to detect unauthorized entry after hours? If so, are they monitored by a security officer or outside agency?			
2.5 Are all external doors alarmed and linked to the main alarm system?			
2.6 Are windows secured with alarms or other intrusion deterrents (bars, wiring, etc.)?			
2.7 Are exit doors reinforced? Are dock doors constructed of materials that prevent unlawful entry?			
2.8 Is lighting both inside and outside the facility adequate to eliminate dark corners?			
2.9 Is flood lighting used on loading and unloading areas? Are dock doors illuminated at night?			
2.10 Are clear zones maintained around the facility? I.e., are brush and growth cleared from the perimeter barrier?			
2.11 Does a guard or receptionist monitor the office entrances?			
2.12 Is there a formal registration process to document visitors to the facility?			
2.13 Is parking for employees separate from the dock and cargo areas?			
2.14 Are containers/trailers that remain at the facility overnight secured and locked/sealed?			
2.15 Are seal numbers verified before trailers or trucks are released from the facility?			
2.16 Is the identification of the truck driver verified before cargo is released to his/her custody?			
2.17 Are truck drivers given limited access to the facility and supervised at all times?			
2.18 Are communication systems in place to contact internal security personnel or local law enforcement officers in the event of an emergency?			

ISUZU

NOTE: We understand that all measures may not be appropriate for the factory because of the company's size and structure. However, the company should strive to implement as many measures as possible to ensure that access to Isuzu's merchandise is restricted to authorized employees.

3. Access Controls

Question	Yes	No	Brief Description of Procedure
3.1 Does the facility have a formal ID system for permanent and temporary employees? Are ID badges with the employee's name and photo issued?			
3.2 Must employees show their badges upon entering the facility?			
3.3 Are badges color-coded to help distinguish workers' assigned areas?			
3.4 Is access to loading docks limited to those employees approved or scheduled to work on the loading docks?			
3.5 Is there a controlled access gate to monitor activity coming in and out of the facility?			
3.6 Is there a formal registration process for visitors?			
3.7 Do employees escort visitors while in a loading facility or warehouse?			
3.8 Do employees or security personnel challenge unknown persons in the facility?			
3.9 Are computers and networks containing sensitive data secured to prevent unauthorized access to such data? Are they password-protected?			
3.10 If information is available in the public domain (e.g., the Internet), is it protected by a firewall?			
3.11 Is access to sensitive information limited to those employees who must access the information to perform their jobs?			
3.12 Is a log of access rights maintained? If an employee separates from the company, are access rights revoked?			
3.13 Is there a procedure in place to ensure that access rights are revoked if an employee separates from the company?			

ISUZU

NOTE: We recognize that many of the standards listed below are the common practice in the U.S., though this might not be the case in the foreign countries in which we operate. We also recognize that some data or information that is available in the U.S. may not be available in other countries.

4. Personnel Security

4. Personnel Security			
Question	Yes	No	Brief Description of Procedure
4.1 Are prospective employees (permanent, temporary, and contract) pre-screened before employment?			
4.2. Are background checks performed on the following areas:			
4.2.1 Criminal convictions?	<input type="checkbox"/>	<input type="checkbox"/>	
4.2.2 Application verification?	<input type="checkbox"/>	<input type="checkbox"/>	
4.2.3 Prior employment?	<input type="checkbox"/>	<input type="checkbox"/>	
4.2.4 Address verification?	<input type="checkbox"/>	<input type="checkbox"/>	
4.3 Are photographs of employees held on file?			

5. Education and Awareness Training

5. Education and Awareness Training			
Question	Yes	No	Brief Description of Procedure
5.1 Does your facility have a formal training program on security awareness?			
5.2 Does the training program address the following areas?			
5.2.1 Recognizing internal conspiracies	<input type="checkbox"/>	<input type="checkbox"/>	
5.2.2 Maintaining product integrity	<input type="checkbox"/>	<input type="checkbox"/>	
5.2.3 Discovering and addressing unauthorized access of the facility or information	<input type="checkbox"/>	<input type="checkbox"/>	
5.3 Is the training conducted within the first 30 days of an employee's tenure?			
5.4 Is the training program included in the facility's self-audit program?			
5.5 Have incentives been established to encourage employees to actively participate in security programs and communicate potential security issues involving theft, conspiracy, or terrorist activities?			