



Annual Report on Forced Labour in Canadian Supply Chains

COA, Inc.

Reporting Year: 2024

Prepared: May 2025



Introduction

As required by Public Safety Canada under *Bill S-211, An Act to enact the Fighting Against Forced Labour and Child Labour in Supply Chains Act and to amend the Customs Tariff* (the “Act”), COA, Inc. has prepared the following report with respect to its activities and supply chains in conjunction with the issue of forced labor. This report has been prepared to the best of the company’s knowledge, having exercised reasonable diligence and the information contained herein is true, accurate and complete for the reporting year 2024.

Background

COA, Inc., DBA Coaster Company of America (“Coaster” or “the Company”) is a U.S based C-Corporation incorporated under the laws of California in 1981. Coaster is a furniture wholesaler and distributor that primarily sources furniture from third party manufacturers and vendors in Asia. The company primarily sells to furniture retailers in the United States of America, with limited sales to Canada.

In 2024, Coaster had six branch and satellite branch operations within the United States, including locations in Northern and Southern California, Illinois, Texas, New Jersey, and Florida. These branch operations service customers in will-call, shipping, and ECOMM channel business. The company does not have physical presence in Canada.

Coaster engages with multiple third-party vendors (“suppliers,” or “manufacturers”) to procure furniture from countries such as China, Vietnam, and Malaysia. The company does not manufacture furniture itself. Coaster engages the services of related party affiliates to perform quality control and logistics services in procuring furniture product from the above-listed countries, including requiring on-site inspections of factory production.



Forced Labor

To reduce the risk of forced labor, the company has conducted an internal assessment of risks of forced labor and/or child labor in its supply chains and activities. Coaster requires its suppliers to comply with local laws on forced labor and child labor and vets suppliers prior to engaging in business with them.

As part of its vendor screening process, Coaster undertakes a vendor questionnaire to ascertain whether a vendor produces furniture product wholly or in part by prohibited forms of labor such as slave, convict, forced labor, or child labor. The questionnaire for each vendor is documented and saved in the company's files. A sample questionnaire is included in this report. Additional documentation is available upon request.

The company also routinely dispatches quality control inspection agents to its vendors' sites.

There have been no instances of identified forced labor or child labor within the company's activities or supply chain as of the date of this report. Consequently, the company has not had to take any steps toward remediation. The company continues to monitor new guidance and legislation on forced labor and/or child labor and is developing training and awareness materials for its staff.

Continued on following page



Attestation

In accordance with the requirements of the Act, and in particular section 11 thereof, I attest that I have reviewed the information contained in the report for the entity or entities listed above. Based on my knowledge, and having exercised reasonable diligence, I attest that the information in the report is true, accurate and complete in all material respects for the purposes of the Act, for the reporting year listed above.”

Lisa Kao
Chairperson
May 31, 2025

Signature: _____

A handwritten signature in blue ink, written over a horizontal line. The signature is stylized and appears to be "Lisa Kao".

I have the authority to bind COA, Inc.



**SAMPLE: BUSINESS PARTNER
SECURITY PROFILE QUESTIONNAIRE**

Business Partner Security Profile Questionnaire for Coaster Company of America

Business Partner Company Information

Company Name:			
Address:			
City, State, Zip			
Country:			
Contact Name:		Title:	
Telephone:		FAX:	
Email:		Website:	
Goods or Services Provided:	Manufacturing and Sales of Furniture		
Years in Business:		Years at This Address:	
Federal Tax ID#: (USA Only)			
FMC or CBP ID # (USA Only)			
Date:			

Business Partner Facility (Site) Information

Building Owner's Name:			
Building Description:			
Type of Construction:			
Office Location in Building:			
Building Size (Sq Ft):		Office Size (Sq Ft):	
# of Building Windows:		# of Office Windows:	
# of Building Doors:		# of Office Doors:	
# Cargo Bays (Street):		# of Cargo Bays (Yard):	
# of Employees in Partner Office:		# of Warehouse Employees:	
Hours of Warehouse Operation:		Hours of Office Operation:	

Corporate Security

1. Security Vision and Responsibility

	REQUIREMENT	YES	NO	N/A	COMMENTS
1	The Company promotes a culture of security and has in place a robust Supply Chain Security Program				
2	Upper Management has demonstrated their commitment to supply chain security and the Importer of Record's CTPAT Participation - by signing a statement of support for the program				
3	A representative from all relevant departments has been appointed to a cross functional team, in support of a robust, Company, supply chain security program				
4	The Company's Supply Chain Security Program is designed with, supported by, and implemented by an appropriate written review component - that holds personnel accountable for their responsibilities				
5	The Company's points of contact (POC) to the Importer of Record are all knowledgeable about CTPAT Program requirements and provide upper management with regular updates on issues related to the program				

2. Risk Assessment

	REQUIREMENT	YES	NO	N/A	COMMENTS
1	There is a process in place to determine any potential risks or where security vulnerabilities may exist within the Company's Supply Chain				
2	Any international portion of the risk assessment should document, or map, the movement of the Company's cargo throughout its supply chain - from the point of origin to the importer's distribution center				

3	Risk assessments are reviewed annually, or more frequently as risk factors dictate				
4	Process and procedures are in place to address management of crisis situations, such as: a security review/recovery plan, a disaster recovery plan, as well as business continuity and resumption plans				

3. Business Partner Requirements

	REQUIREMENT	YES	NO	N/A	COMMENTS
1	The Company has a written, risk based, process for screening new business partners and for monitoring current partners				
2	The business partner screening process takes into account whether a partner is a CTPAT member, or a member in an Approved Economic Operator (AEO) program with a Mutual Recognition Arrangement (MRA) with the United States				
3	The Company, whenever outsourcing or contracting parts of its supply chain, conducts due diligence (via visits or questionnaires) to ensure their business partners have security measures in place that meet or exceed CTPAT Minimum Security Criteria (MSC)				
4	The Company directs weaknesses, identified in business partners' security assessments, to be addressed as soon as possible, and corrections implemented in a timely manner				
5	The business partner selection process includes investigating potential activities related to money laundering and terrorist funding				
6	A process is in place to closely examine business partners to ensure sourced goods/services are not mined, produced or manufactured wholly or in part with prohibited forms of labor: such as, slave, convict, forced labor or forced child labor				
7	The Company ensures its business partners continue to comply with CTPAT's security criteria by updating their security assessments of their business partners on a regular basis, or as circumstances/risks dictate				

4. Cybersecurity

	REQUIREMENT	YES	NO	N/A	COMMENTS
1	The Company has a comprehensive, witten, cybersecurity procedure to protect all Infomation Technology (IT) Systems.				
2	All Company computers and systems are protected by software and/or hardware firewalls that detect and prevent attempted illicit intrusion, alteration of data, and unauthorized access to data - and these efforts are updated regularly				
3	The Company's IT infrastructure and network systems are regularly tested for security. If vulnerabilities are found, corrective actions are taken as soon as possible				
4	The Company has a process in place to both communicate and share any cyber threats with Government authorities and business partners				
5	The Company has a system in place to identify unauthorized access of IT systems/data or abuse of policies and procedures - including improper access of internal systems or external websites and tampering or altering of business data by employees or contractors				
6	Cybersecurity policies and procedures are reviewed annually, or more frequently, as risk or circumstances dictate				

7	User access is restricted based upon job description, or assigned duties and is reviewed on a regular basis to ensure access to sensitive systems is based on job requirements				
8	All of the Company IT systems are password protected with access granted to authorized users with individually assigned accounts. Passwords are changed periodically. (Describe frequency of password change in comments section. Is it changed every 30, 60, or 90 days, etc...)				
9	If the Company has "remote" users that connect to their network, they utilize secure technologies, such as a Virtual Private Network (VPN) to allow employees to access the company's intranet securely when outside Company offices				
10	If the Company allows employees to use personal devices to conduct Company work, all such devices adhere to the Company's cybersecurity policies and procedures, to include updates				
11	Cybersecurity policies and procedures include measures to prevent the use of counterfeit or improperly licensed technology products				
12	Data is backed up once a week, or as appropriate. All sensitive and confidential data should be stored in an encrypted format				
13	All media, hardware, or other IT equipment that contains sensitive information regarding import/export process is accounted for through regular inventories				

Transportation Security

5. Conveyance and Instruments of International Traffic Security

	REQUIREMENT	YES	NO	N/A	COMMENTS
1	All conveyances and Instruments of International Traffic (IIT) are stored in a secure area to prevent unauthorized access				
2	The CTPAT inspection process has written procedures for both security and agricultural inspections				
3	Containers: Procedures are in place to verify the physical integrity of the container structure prior to stuffing, to include the reliability of the locking mechanisms of the doors. A 7 point inspection process is conducted for all containers. This inspection process includes the Front wall, Left side, Right side, Floor, Ceiling/Roof, Inside/outside doors, and Outside/Undercarriage.				
4	Tractor - Trailers: Procedures are in place to verify the physical integrity of the trailer, as well as the tractor, prior to stuffing - to include the reliability of the locking mechanisms of the doors. A 17 point inspection process is conducted for all tractor/trailers. This inspection includes Bumper, Engine, Tires, Floor, Fuel Tanks, Cab, Air Tanks, Drive Shafts, Fifth Wheel, Outside/Undercarriage, Floor (inside trailer), Inside/Outside doors, Side Walls, Ceiling/Roof, Front Wall, Refrigerator Unit and Exhaust.				
5	Conveyances and Instruments of International Traffic (as appropriate) are equipped with external hardware that can reasonably withstand attempts to remove it. This includes doors, handles, rods, hasps, rivets, brackets, and locking mechanisms that can be inspected to detect tampering and/or any hardware inconsistencies - prior to the attachment of any sealing device				
6	The inspection of all conveyances and empty Instruments of International Traffic are recorded on a checklist, such as container/conveyance number; date of inspection; time of inspection; name of inspector(s); as well as areas of inspection				

7	All security inspections are performed in an area of controlled access and, if available, monitored via a CCTV system				
8	Based upon risk, Company management personnel conduct random searches of conveyances after the transportation staff have conducted conveyance inspections				
9	The Company works with its transportation providers to track conveyances from origins to final destination points.				
10	For land border shipments, that are in proximity to the United States border, a "no stop" policy has been implemented with regard to unscheduled stops				
11	If a credible (or detected) threat to the security of a shipment or conveyance is discovered, the Company has a process in place to alert (as soon as reasonably possible) any business partners in its supply chain that may be affected - as well as law enforcement authorities				

6. Seal Security

	REQUIREMENT	YES	NO	N/A	COMMENTS
1	Written procedures are in place to stipulate how seals are to be controlled and affixed to loaded containers or trailers - to include procedures for recognizing and reporting compromised seals to US Customs and Border Protection - or the appropriate foreign authority.				
2	At point of stuffing, procedures are in place to properly seal and maintain the integrity of the shipping containers while they are in the custody of the carrier or the facility where the shipment is being made from. (Describe these procedures in the comments section.)				
3	A high security seal is affixed to all loaded containers or trailer conveyances bound for the United States. These seals meet or exceed the current PAS ISO 17712 standards for high security seals. (Describe who supplies and controls the seals.)				
4	A process is in place to verify that high security seals (bolt/cable) have been affixed properly to Instruments of International Traffic - and are functioning as designed. (Describe the process)				
5	Only designated/trained employees are allowed to utilize/affix/inspect seals - for integrity purposes. (Describe who is authorized to handle container seals and what type of training they receive.)				
6	Written procedures are in place and in use to maintain container integrity and to protect against the introduction of unauthorized material and/or persons while containers are in the custody of this facility or carrier.				
7	If a seal is found to be compromised, broken or otherwise altered while a container/trailer is being delivered to this carrier or facility, a procedure is in place to determine when the seal was broken or changed. (Describe this procedure.)				
8	If representatives of this carrier or facility are unable to determine who compromised or replaced a seal before it was delivered into their custody - or while it was in their custody - procedures are in place to open the container and inspect its contents. The nature of the situation will determine whether this task should be performed by the carrier, those in the facility, or by law enforcement personnel. (Describe who would perform this investigation and the circumstances that determine who will do it.)				

9	Procedures are in place to inform US Customs or other, appropriate, law enforcement organizations of the discovery of a broken or changed seal if the parties for breaking or changing the seal are identified or unauthorized. (Describe these procedures.)				
10	Procedures are in place to notify customers and other parties involved in the movement of a conveyance/container found to have a broken or changed seal. This notification includes the circumstances surrounding the discovery of the broken or altered seal, and the results of any subsequent investigations and container content checks.				
11	Procedures are in place for reporting and neutralizing unauthorized entry into containers or container storage areas. (Describe these procedures.)				

7. Procedural Security

	REQUIREMENT	YES	NO	N/A	COMMENTS
1	All cargo staged overnight, or for an extended periods of time, is secured from unauthorized access				
2	All cargo staging areas and surroundings are inspected on a regular basis to ensure these areas remain free of visible pest contamination				
3	The loading/stuffing of cargo into containers/IIT is supervised by a security officer, manager, or other specifically designated personnel				
4	As documented evidence of the properly installed seal, digital photographs are taken at the point of stuffing. To the extent feasible, these images are electronically forwarded to the shipment destination for verification purposes				
5	Procedures are in place to ensure that all information used in clearing of cargo is legible, complete, accurate and protected against the exchange, loss, or introduction of erroneous information, and reported on time				
6	If paper documents are being used, forms and other import/export related documentation is secured to prevent unauthorized use				
7	The shipper, or its agent ensures that the Bill of Ladings (BOL) and/or manifests accurately reflect the information provided to the carrier, and the carrier exercises due diligence to ensure these documents are accurate				
8	All Bills of Lading are filed with U.S. Customs in a timely fashion, and in a manner as required				
9	Bill of Lading information filed with U.S. Customs clearly indicates the first foreign location/facility where the carrier has taken possession of the cargo destined for the United States				
10	Personnel are trained on how to identify information in shipping documents, such as manifests, that might indicate a suspicious shipment. (Explain training in comments section)				
11	This facility has written procedures in place to identify, handle, and report unmanifested or improperly manifested cargo. (Explain in comments section)				
12	A notification protocol is in place to report any suspicious activities or security incidents (such as drug seizures, discovery of stowaways, etc) that take place anywhere around the world and which affects the security of the Company's supply chain				

13	All shortages, overages and other significant discrepancies or anomalies are investigated and resolved as appropriate				
14	Procedures are in place to identify, challenge, and address unauthorized/unidentified persons on the site grounds, and especially in cargo handling areas, as well as how to respond to that type of discovery situation				
15	All arriving cargo is reconciled against information on the cargo manifest				
16	All departing cargo is verified against purchase or delivery orders				
17	Seal numbers assigned to specific shipments are transmitted to the consignee prior to departure				
18	Seal numbers are electronically printed on Bills of Lading, or other shipping documents				
19	The Company has written procedures for reporting security incidents, which includes a description of the facility's internal escalation process. (review procedures in comments section)				
20	Notification procedures include the accurate contact information that lists the name(s) and phone number(s) of personnel requiring notification, as well as appropriate law enforcement agencies				
21	The Company initiates their own internal investigations of any security related incidents (terrorism, narcotics, stowaways, absconders, etc.) immediately after becoming aware of any security related incident				
22	All internal Company investigations are documented, completed as soon as is feasibly possible, and made available to CBP/CTPAT and any other law enforcement agency, as appropriate, upon request				
23	The Company has a process in place to ensure that any/all physical documents, related to freight movements, are kept secure. (Describe this process in the comments section)				

8. Agricultural Security

	REQUIREMENT	YES	NO	N/A	COMMENTS
1	There processes and procedures in place designed to prevent visible contamination - including compliance with Wood Packaging Materials (WPM)				
2	The Company complies with the requirements established on the Standards for Phytosanitary Measures No. 15 (ISPM 15) to help prevent the spread of pests and diseases carried over on wood packaging being transported				
3	The Company has implemented measures such as vacuuming, sweeping with brooms, or clearing with blowers to help to eliminate contaminants in containers/conveyances				
4	There are processes in place to ensure Containers/Trailers are clean prior to loading.				

People & Physical Security

9. Physical Security

	REQUIREMENT	YES	NO	N/A	COMMENTS
1	All cargo handling and storage facilities, including trailer yards and offices, have physical barriers and/or deterrents that prevent unauthorized access				
2	Perimeter fencing encloses the areas around cargo handling and storage facilities				

3	If the facility handles cargo, internal fencing/delineations are used to secure cargo and cargo handling areas				
4	Fencing is regularly inspected for integrity and damage by designated personnel				
5	Gates, where vehicles and/or personnel enter or exit (as well as other points of egress) are either manned or monitored				
6	Private vehicles are prohibited from parking in or adjacent to cargo handling and storage areas, as well as conveyances				
7	Adequate lighting is provided both inside and outside the facility including, as appropriate, the following areas: entrances and exits, cargo handling and storage areas, fence lines, and parking areas				
8	Security technology is used to monitor the premise/facility - to prevent unauthorized access to sensitive areas				
9	Electronic burglary alarm systems are in use (describe the brand of technology and what areas are protected in comments section)				
10	Electronic access control systems are in use (describe the brand of technology and what areas are protected in comments section)				
11	Video surveillance systems are in use (CCTV). (describe the type, components, number of cameras, and recording frame rate in comments section)				
12	If technology is being utilized, access to the locations where it is controlled or managed is limited to authorized persons				
13	If technology is utilized, procedures have been implemented to test/inspect the technology on a regular basis				
14	If technology is being utilized, inspections include verifications that all of the equipment is positioned appropriately and working properly				
15	If technology is being utilized, the results of inspections and performance testing is documented, as well as any corrections/modifications made				
16	Results of any technology inspections are maintained for a sufficient time for audit purposes				
17	The Company utilized licensed/recognized resources when it considered the design and installation of its security technology				
18	Security technology systems are configured with an alternative power source that will allow the systems to continue to function in the event of an unexpected power loss				
19	If video surveillance systems (CCTV) are being used, the cameras are positioned to cover key areas of the facility that pertain to import/export processes				
20	If video surveillance systems (CCTV) are being used, they are programmed to record at the highest picture quality setting reasonably available, and set to record 24/7				
21	If video surveillance systems (CCTV) are being used, the cameras/recorders have an alarm/notification feature which signals when a failure to operate or record occurs				

22	If video surveillance systems (CCTV) are being used, periodic, random reviews of the recorded footage are conducted (by management, security, or other designated personnel) to verify that cargo security procedures are being properly followed. Brief, written summaries, are recorded for each review				
23	If video surveillance systems (CCTV) are being used, recordings of footage coverage key import/export processes is maintained on monitored shipments for a sufficient time to allow for an investigation to be completed				
24	Security guards patrol the interior and exterior of the building. (Describe the hours and areas patrolled when guards are used.)				
25	All building doors, windows, walls, gates, and fences are inspected on a regular basis (Note frequency in comments section.)				
26	All physical security breaches are reported to management - and to local authorities - when they are discovered.				
27	All office space in the facility is capable of being secured in a manner that prevents uncontrolled access between warehouse and office space. (Describe how this is done in comments section.)				
28	There is a documented Site Security Plan in place for the measures taken to physically secure the facility.				

10. Physical Access Controls

	REQUIREMENT	YES	NO	N/A	COMMENTS
1	Where applicable, a personnel identification process/system is in place for positive identification and access control purposes				
2	There are written procedures governing how identification badges and access devices are granted, changed, or revoked. (Produce copy of the procedures)				
3	Access to sensitive areas is restricted based on job description and assigned duties				
4	Removal of all access privileges takes place whenever an employee separates from the company - either by personal choice or Company direction				
5	Visitors, vendors and service providers are required to present photographic identification upon arrival				
6	A log is maintained of all visitor, vendor, or service provider visits to the facility. The log includes the date of visit, time of the visit, visitor's name, verification of identification, company point of contact, as well as time of departure. (Produce the log for inspection)				
7	All visitors, vendors and/or service providers are issued a temporary identification				
8	All visitors are escorted within the facility				
9	Drivers, delivering or receiving cargo, are positively identified by presenting a government-issued form of identification - before cargo is received or released				

10	A cargo pick-up log is kept to register the driver and conveyance information when cargo is being picked-up. The log collects, at a minimum, the following information: - Driver's Name - Date and time of Arrival - Company Name - Truck & Trailer Number - Time of Departure - Seal Number affixed to the shipment				
11	Prior to arrival the incoming carrier notifies the facility of the estimated time of arrival for the scheduled pick-up, the name of the driver, and the truck number				
12	Arriving packages and mail are periodically screened for contraband before being admitted				
13	If security guards are being utilized, work instructions, such as Post Orders, are contained within written policies and procedures (Produce written police & procedures)				
14	If security guards are being utilized, Company management periodically verifies compliance and appropriateness with these procedures through audits and policy reviews				
15	Restricted areas are marked.				
16	Access to restricted areas is controlled. (Describe these controls in the comments section)				
17	This facility has an incentive system for reporting unauthorized access				
18	This facility has an incentive system for challenging unauthorized personnel				

11. Personnel Security

	REQUIREMENT	YES	NO	N/A	COMMENTS
1	Written processes are in place to screen prospective employees (Produce written processes)				
2	Application information, such as employment history and references, is verified prior to hire, to the extent possible and allowed by law				
3	In accordance with applicable legal limitations, and the availability of criminal record databases, employee background screening is conducted				
4	Once employed, periodic re-investigations are conducted based on either random selection, specific acts of cause, or the sensitivity of the employee's position				
5	Based on the sensitivity of the position, employee vetting requirements are extended to all temporary workforce employees and to contractors				
6	The Company has an Employee Code of Conduct that includes expectations and defines acceptable behaviors (Produce Code of Conduct)				
7	Penalties and disciplinary procedures are included in the Employee Code of Conduct				
8	Employees acknowledge that they have read and understand the Code of Conduct by signing it and the signature is maintained in the employee's file for documentation				

12. Education, Training and Awareness

	REQUIREMENT	YES	NO	N/A	COMMENTS
--	-------------	-----	----	-----	----------

1	A security training and awareness program exists to recognize and foster awareness of the security vulnerabilities to facilities, conveyances and cargo - at each point in the supply chain which could be exploited by terrorists or contraband smugglers (Produce evidence of program)				
2	The security training and awareness program covers the CTPAT security requirements				
3	New Company employees, where applicable, receive security and awareness training as a part of their orientation/job skills training				
4	Evidence of security training and awareness is maintained in training logs, sign-in sheets, or electronic training records. (Produce evidence of training)				
5	Employees, drivers, and other personnel who conduct security inspections of conveyances, and Instruments of International Traffic, are trained in how to conduct those inspections, as well as what to look for - such as hidden compartments, concealed contraband, and signs of pest contamination				
6	The Company has measures in place to verify that the training provided meets all of the training objectives				
7	Specialized training is provided annually to personnel who may be able to identify the CTPAT warning indicators of "trade-based" money laundering and terrorism financing				
8	As applicable, based on employee function or position, personnel are trained on the company's cybersecurity policies and procedures - to include the need for employees to protect passwords, passphrases, and computer access				
9	Personnel operating and/or managing security technology systems receive operations and maintenance training in their specific areas. (Self-training via operational manuals and other methods is acceptable)				
10	Personnel are trained on how to report security incidents and suspicious activities				
11	Training, in accordance with the Company business model, is provided to applicable personnel on preventing visible pest contamination				