V OPCO, LLC C-TPAT QUESTIONNAIRE FOR FACTORIES

Company: ____

Address: ____

		Minimum Security Criteria Requirement (Must/Should)		
General Security			*(YES OR NO)*	
▶	Factory has a written security plan. **If yes, please provide a copy of the Factory Security Manual and/or written procedures.*	MUST		
▶	Factory has a designated security officer. **If yes, please provide name and contact information:*	MUST		
▶	Factory maintains copies of the third party audits/inspections of plant factory.	SHOULD		
1. Security, Vision, and Responsibility *(only applicable to C-TPAT members in Canada and Mexico)*			*(YES OR NO)*	
1.1	Factory demonstrates its commitment to supply chain security and the security program through a statement of support, which is signed by a senior company official and displayed in appropriate company locations.	SHOULD		
1.2	Factory incorporates representatives from all of the relevant departments into a cross-functional Supply Chain Security team.	SHOULD		
1.3	The supply chain security program are designed with, supported by, and implemented by an appropriate written security policies and procedures. These policies and procedures are updated as needed based on pertinent changes in an organization's operations and level of risk.	MUST		
1.4	Factory's Point(s) of Contact (POC) to security must be knowledgeable about security program requirements.	MUST		
2. Risk Assessment *(only applicable to C-TPAT members in Canada and Mexico)*			*(YES OR NO)*	
2.1	Factory conducts an overall risk assessment to identify where security vulnerabilities may exist in their supply chains annually or more frequently as risk factors dictate.	MUST		
2.2	The international portion of the risk assessment documents or maps the movement of the factory's cargo throughout its supply chain from the point of origin to the importer's distribution center.	SHOULD		
2.3	Factory performs periodic security assessments.	MUST		
2.4	Factory has written procedures in place that address crisis management, business continuity, security recovery plans and business resumption.	SHOULD		
3. Business Partners			*(YES OR NO)*	
3.1	Factory has a written, risk-based process for screening new business partners and for monitoring current partners. Factory should also include in this process checks on activity related to money laundering and terrorist funding.	MUST		
3.2	Factory's business partner screening process should take into account whether a partner is a CTPAT member or a member in an approved Authorized Economic Operator (AEO) program with a Mutual Recognition Arrangement (MRA) with the United States (or an approved MRA). Factory obtains evidence of the certification from the business partner(s) and are continuously monitored to ensure they maintain their certification.	MUST		
3.3	Factory exercises due diligence (via visits, questionnaires, etc.) to ensure their business partners have security measures in place that meet or exceed CTPAT's Minimum Security Criteria (MSC).	MUST		
3.4	Weaknesses identified during business partners' security assessments are addressed and corrections are implemented in a timely manner. Factory requires documentary evidence be provided to confirm deficiencies have been corrected.	MUST		
3.5	Factory performs security assessments of business partners at least annually or more frequently as circumstances/risks dictate.	SHOULD		
3.6	For inbound shipments to the United States, if a factory subcontracts transportation services to another highway carrier, the factory must use a CTPAT certified highway carrier or a highway carrier that works directly for the factory as delineated through a written contract. The contract must stipulate adherence to all minimum security requirements. ****Only applicable for inbound shipments from Canada and Mexico*	MUST		
3.7	Factory has a documented social compliance program in place that, at minimum addresses how the company ensures goods imported into United States were not mined, produced or manufactured, wholly or in part, with prohibited forms of labor, e.g. forced, imprisoned, indentured or indentured child	SHOULD		
4. Cybersecurity including Information Technology			*(YES OR NO)*	
4.1	Factory has comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems. The written IT policy, at a minimum, must cover all of the individual Cybersecurity criteria.	MUST		
4.2	To defend Information Technology (IT) systems against common cybersecurity threats, factory must install sufficient software/hardware protection from malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewalls) in their computer systems. Factory must ensure their security software is current and receives regular security updates.	MUST		
4.3	Factory must also have policies and procedures in place to prevent attacks via social engineering. If a data breach occurs or another unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and/or data.	MUST		
4.4	Factory must regularly test the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.	MUST		
4.5	Factory's cybersecurity policies or procedures address how factory shares information on cybersecurity threats with the government and other business partners.	SHOULD		
4.6	Factory must have 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 with or altering of business data by employees or contractors. All violators must be subject to appropriate disciplinary actions.	MUST		
4.7	Cybersecurity policies and procedures must be reviewed annually, or more frequently, as risk or circumstances dictate. Following the review, corrective actions are implemented in a timely manner if vulnerabilities are found.	MUST		
4.8	Factory has policies in place to restrict user access based on job description or assigned duties. Authorized access must be reviewed on a regular basis to ensure access to sensitive systems is based on job requirements. Computer and network access must be removed upon employee separation.	MUST		
4.9	Factory requires individuals with access to Information Technology (IT) systems to use individually assigned accounts.	MUST		
4.10	Factory uses strong passwords, passphrases, or other forms of authentication, to protect IT systems from infiltration. User access to IT systems must be safeguarded at all times.	MUST		
4.11	Factory requires passwords and/or passphrases be changed as soon as possible if there is evidence of compromise or reasonable suspicion of a	MUST		
4.12	Factory must employ secure technologies, such as virtual private networks (VPNs) to allow employees who must connect remotely to access the company's intranet securely when located outside of the office. Factory must also have procedures designed to prevent remote access from	MUST		
4.13	If factory allows their employees to use personal devices to conduct company work, all such devices must adhere to the company's cybersecurity policies and procedures to include regular security updates and a method to securely access the company's network.	MUST		
4.14	Cybersecurity policies and procedures include measures to prevent the use of counterfeit or improperly licensed technological products.	SHOULD		
4.15	Factory's data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format.	SHOULD		
4.16	All media, hardware, or other IT equipment that contains sensitive information regarding the factory's import/export process are accounted for through regular inventories. When disposed, they must be properly sanitized and/or destroyed in accordance with the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization or other appropriate industry guidelines.	MUST		
5. Conveyance and Instruments of International Traffic Security (Container Security)			*(YES OR NO)*	
5.1	Factory has written procedures in place detailing the storage of containers and trucks -- both empty and full -- in a secured area to prevent unauthorized	MUST		
5.2	Factory has written procedures for both security and agricultural inspections of containers, trucks, or other conveyances and Instruments of International Traffic (IIT).	MUST		

5.3	Prior to loading/stuffing/packing, factory requires all conveyances and empty IIT undergo CTPAT approved security and agricultural inspections to ensure their structures have not been modified to conceal contraband, or have not been contaminated with visible agricultural pests. Inspection requirements for CTPAT shipments via ocean, air, and land borders (as applicable) by rail or intermodal freight include an eight-point inspection on all containers and ULDs prior to loading/stuffing. The follow items should be checked: 1. Front wall 2. Left side 3. Right side 4. Floor 5. Ceiling/Roof 6. Inside/outside doors, including the reliability of the locking mechanisms of the doors; 7. Outside/Undercarriage 8. Check for pests	MUST		
5.4	For land border crossings via highway carriers, additional inspection requirements include inspections of containers and trucks at conveyance/IIT storage yards. When possible, inspections are conducted upon entering/departing the storage yard and at the point of loading/stuffing. These systematic inspections must include 17-point inspections: **Tractors** 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 7. Faring/roof **Trailers** 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 mechanism 10. Outside/Undercarriage	MUST		
5.5	Factory must utilize containers and trucks equipped with external hardware that can reasonably withstand attempts to remove it or tamper with. The door, handles, rods, hasps, rivets, brackets, and all other parts of a container's locking mechanism must be fully inspected to detect tampering and any hardware inconsistencies prior to the attachment of any sealing device	MUST		
5.6	Factory records all inspections of containers and trucks on a checklist. The following elements should be documented on the checklist: • Container/Trailer/Instruments of International Traffic number; • Date of inspection; • Time of inspection; • Name of employee conducting the inspection; and • Specific areas of the Instruments of International Traffic that were inspected. If the inspections are supervised, the supervisor should also sign the checklist. The completed container/Instruments of International Traffic inspection sheet should be part of the shipping documentation packet. The consignee should receive the complete shipping documentation packet prior to receiving the merchandise.			
5.7	Factory performs all security inspections in an area of controlled access and, if available, monitored via a CCTV system.	SHOULD		
5.8	If visible pest contamination is found during the containers and trucks inspection, washing/vacuuming must be carried out to remove such contamination. Factory must retain documentation for one year to demonstrate compliance with these inspection requirements.	MUST		
5.9	Factory management personnel should conduct random searches on containers and trucks once every 2-3 months after transportation staff have conducted conveyance/IIT inspection checks. The searches should be conducted at random without warning, so they will not become predictable. The inspections should be conducted at various locations where the conveyance is susceptible: the carrier yard, after the truck has been loaded, and en route to the United States border.	SHOULD		
5.10	Factory should work with their transportation providers to track conveyances from origin to final destination point. Specific requirements for tracking, reporting, and sharing of data should be incorporated within terms of service agreements with service providers.	SHOULD		
5.11	Factory should have access to their carrier's GPS fleet monitoring system so they may track the movement of their shipments.	SHOULD		
5.12	For land border shipments that are in proximity to the United States border, a "no-stop" policy should be implemented with regard to unscheduled stops. ****Only applicable for inbound shipments from Canada and Mexico*	SHOULD		
5.13	In areas of high risk, and immediately prior to arrival at the border crossing, factory should incorporate a "last chance" verification process for U.S. bound shipments for checking of containers or trucks for signs of tampering to include visual inspections of conveyances and the VVTT seal verification process. Properly trained individuals should conduct the inspections.	SHOULD		
5.14	Factory has procedures in place for notifying business partners in the supply chain that may be affected and law enforcement agencies, as appropriate, if a credible (or detected) threat to the security of a shipment or conveyance is discovered.	MUST		
6. Seal Security			*(YES OR NO)*	
6.1	Factory has detailed, written high security seal procedures that describe how seals are issued and controlled at the factory and during transit. Procedures must provide the steps to take if a seal is altered, tampered with, or has the incorrect seal number, including documentation of the event, communication protocols to partners, and investigation of the incident. The findings from the investigation must be documented, and any corrective actions must be implemented as quickly as possible.	MUST		
6.2	Written procedures must be maintained at the local operating level so that they are easily accessible. Procedures must be reviewed at least once a year and updated as necessary.	MUST		

6.3	Written seal controls must include the following elements: **Controlling Access to Seals** • Management of seals is 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. • Only trained, authorized personnel may affix seals to containers. **Controlling Seals in Transit** • When picking up sealed IIT (or after stopping) verify the seal is intact with no signs of tampering. • Confirm the seal number matches what is noted on the shipping documents. **Seals Broken in Transit** • If a load is examined, record the replacement seal number. • The driver must immediately notify dispatch when a seal is broken, indicate who broke the seal, and provide the new seal number. • The carrier must immediately notify the shipper, broker, and importer of the seal change and the replacement seal number. • The shipper must note the replacement seal number in the seal log. **Seal Discrepancies** • Retain altered or tampered seals to aid in investigations. • Investigate the discrepancy; follow-up with corrective measures (if warranted). • As applicable, report compromised seals to CBP and the appropriate foreign government to aid in the investigation.	MUST		
6.4	All international shipments are secured immediately after loading/stuffing/packing by the responsible party (ie. factory or authorized packer acting on factory's behalf) with a high security seal that meets or exceeds the most current ISO 17712 standard for high-security seals. Factory must ensure that all seals used must be securely and properly affixed to containers.	MUST		
6.5	Factory must document and maintain all seal audit logs. Annual seal audits, conducted by either a factory manager or a security supervisor, must include periodic inventory of stored seals and reconciliation against seal inventory logs and shipping documents. As part of the overall seal audit process, dock supervisors and/or warehouse managers must periodically verify seal numbers used on containers.	MUST		
6.6	Factory seal verification process ensures all high-security seals such as bolts and cables are affixed properly to all containers and are operating as designed. Factory follows below 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.	MUST		
7. Procedural Security			*(YES OR NO)*	
7.1	Factory must ensure cargo is secure from unauthorized access when cargo is staged overnight or for an extended period of time.	MUST		
7.2	Factory must ensure cargo staging areas, and the immediate surrounding areas, be inspected at least monthly to makre sure these areas remain free of visible pest contamination.	MUST		
7.3	The loading/stuffing of cargo into containers should be supervised by a security officer/manager or other designated personnel of the factory.	SHOULD		
7.4	Factory should document evidence of the properly installed seal with digital photographs taken at the point of stuffing. To the extent feasible, these images should be electronically forwarded to the destination for verification purposes.	SHOULD		
7.5	Factory has procedures in place to ensure that all information used in the clearing of merchandise/cargo is legible, complete, accurate, protected against the exchange, loss, or introduction of erroneous information, and reported on time.	MUST		
7.6	Unused paper documents, forms, and other import/export related documentation should be secured to prevent unauthorized use.	SHOULD		
7.7	Factory must ensure that bill of ladings (BOLs) and/or manifests accurately reflect the information provided to the carrier, such as weight and piece	MUST		
7.8	Factory must have written procedures for reporting an incident, which includes a description of the factory's internal escalation process. Factory has a notification protocol in place to report any suspicious activities or security incidents that may affect the security of the factory's supply chain. Notification procedures include accurate contact information that lists the name(s) and phone number(s) of factory personnel requiring notification, as well as for law enforcement agencies. Procedures must be annually reviewed to ensure contact information is accurate.	MUST		
7.9	Factory has procedures in place to identify, challenge, and address unauthorized/unidentified persons. Employees must know the protocol to challenge an unknown/unauthorized person, how to respond to the situation, and be familiar with the procedure for removing an unauthorized individual from	MUST		
7.10	Factory should have a protocol in place to report security related issues anonymously. When an allegation is received, it should be investigated, and if applicable, corrective actions should be taken.	SHOULD		
7.11	All shortages, overages, and other significant discrepancies or anomalies are investigated and resolved in a timely manner, as appropriate.	MUST		
7.12	Arriving cargo should be reconciled against information on the cargo manifest. Departing cargo should be verified against purchase or delivery orders.	SHOULD		
7.13	Seal numbers assigned to specific shipments should be transmitted to the consignee prior to departure.	SHOULD		
7.14	Seal numbers should be electronically printed on the bill of lading or other shipping documents.	SHOULD		
7.15	Following a significant security incident, factory must initiate a post-incident analysis immediately after becoming aware of the incident. The results of the factory's post-incident analysis must be documented, completed as soon as possible, and made available to CTPAT Supply Chain Security Specialists (SCSS), if allowed by law enforcement authorities.	MUST		
8. Agricultural Security (*if wood packing materials are used during transportation)*			*(YES OR NO)*	
8.1	Factory has written procedures designed to prevent visible pest contamination to include compliance with Wood Packing Materials (WPM) regulations.	MUST		
8.2	Visible pest prevention measures are adhered to throughout the supply chain.	MUST		
8.3	If Wood Packaging Materials (WPM) are used in the shipping process, they must be debarked and heat treated or fumigated with methyl bromide, stamped or branded with the IPPC (International Plant Protection Convention) mark of compliance.	MUST		
9. Physical Security			*(YES OR NO)*	
9.1	Factory's cargo handling and storage facilities, including trailer yards and offices, have physical barriers and/or deterrents that prevent unauthorized	MUST		
9.2	Perimeter fencing should enclose the areas around cargo handling and storage facilities. If a factory handles cargo, interior fencing should be used to secure cargo and cargo handling areas. Additional interior fencing should segregate various types of cargo such as domestic, international, high value, and/or hazardous materials. Factory should regularly inspect the fencing for signs of tamper or damage by designated factory personnel. Any damage found should be repaired as soon as possible.	SHOULD		
9.3	Factory must have manned security or monitoring at gates where vehicles and/or personnel enter or exit (as well as other access points). Individuals and vehicles may be subject to search in accordance with local and labor laws.	MUST		
9.4	Factory prohibits private passenger vehicles from parking in or adjacent to cargo handling and storage areas, and conveyances.	MUST		
9.5	Factory must have adequate lighting inside and outside of the factory including, as appropriate, the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas.	MUST		
9.6	Security technology such as CCTV, burglary alarm system, and access control devices, should be utilized to monitor premises and prevent unauthorized access to sensitive areas.	SHOULD		

9.7	Factory must have written policies and procedures governing the use, maintenance, and protection of their security technology. At a minimum, these policies and procedures must stipulate: • That access to the locations where the technology is controlled or managed is limited to authorized personnel; • The procedures that have been implemented to test/inspect the technology on a regular basis; • That the inspections include verifications that all of the equipment is working properly, and if applicable, that the equipment is positioned correctly; • That the results of the inspections and performance testing is documented; • That if corrective actions are necessary, they are to be implemented as soon as possible and the corrective actions are documented; • That the documented results of these inspections be maintained for a sufficient time for audit purposes.	MUST		
9.8	If a third party central monitoring station (off-site) is used, factory has written procedures stipulating critical systems functionality and authentication protocols such as (but not limited to) security code changes, adding or subtracting authorized personnel, password revision(s), and systems access or	MUST		
9.9	Factory reviews and updates security technology policies and procedures annually, or more frequently, as risk or circumstances dictate.	MUST		
9.10	Factory should use licensed/certified resources when considering the design and installation of security technology.	SHOULD		
9.11	All security technology infrastructure must be physically secured from unauthorized access.	MUST		
9.12	Factory configures security technology systems with an alternative power source that will allow the systems to continue to operate in the event of an unexpected loss of direct power.	SHOULD		
9.13	If camera systems are deployed, cameras should monitor a factory's premises and sensitive areas to deter unauthorized access. Alarms should be used to alert factory personnel to unauthorized access into sensitive areas.	SHOULD		
9.14	Cameras must be positioned to cover key areas of factory's facilities that pertain to the import/export process. Cameras should be programmed to record at the highest picture quality setting available, and be set to record on a 24/7 basis.	MUST		
9.15	Cameras should have an alarm/notification feature, which would signal a "failure to operate/record" condition.	SHOULD		
9.16	Factory's management, security team, or other designated personnel, must conduct random periodic reviews of the camera footage at least once every 3 months to verify that cargo security procedures are being properly follow. Results of the reviews must be summarized in writing to include any corrective actions taken. Factory must maintain the results for a sufficient time for audit purposes.	MUST		
9.17	Factory should maintain recordings of footage covering key import/export processes for at least 90 days to allow sufficient time for an investigation to	SHOULD		
10. Physical Access Controls			*(YES OR NO)*	
10.1	Factory must have written procedures governing how identification badges and access devices are granted, changed, and removed. A personnel identification system must be in place for positive identification and access control purposes. Access to sensitive areas must be restricted based on job description or assigned duties. Removal of access devices must take place when the employees separate from the company.	MUST		
10.2	Factory must require all visitors, vendors, and service providers to present photo identification upon arrival, and a log be maintained to record the details of the visit. All visitors are to be escorted throughout the facility. Temporary identification such as ID badges are issued to all visitors and are visibly displayed at all times during the visit. The registration log must include the following: • Date of the visit • Visitor's name • Verification of photo identification (type verified such as license or national ID card). Frequent, well known visitors such as regular vendors may forego the photo identification, but must still be logged in and out of the facility. • Time of arrival • Company point of contact • Time of departure	MUST		
10.3	Factory's registration log must include the following: • Date of the visit • Visitor's name • Verification of photo identification (type verified such as license or national ID card). Frequent, well known visitors such as regular vendors may forego the photo identification, but must still be logged in and out of the facility. • Time of arrival • Company point of contact • Time of departure	MUST		
10.4	Factory requires all drivers delivering or receiving cargo present government-issued photo identification to factory security personnel before cargo is received or released.	MUST		
10.5	Factory must maintain a cargo pickup log to register drivers and record the details of their conveyances when picking up cargo. The cargo log must be kept secured, and drivers must not be allowed access to it.	MUST		
10.6	The cargo pickup log must have the following items recorded: • Driver's name • Date and time of arrival • Employer • Truck number • Trailer number • Time of departure • The seal number affixed to the shipment at the time of departure	MUST		
10.7	Prior to arrival, the carrier are required to notify the factory of the estimated time of arrival for the scheduled pick up, the name of the driver and truck	SHOULD		
10.8	Factory should periodically screen arriving packages and mail for contraband before being admitted.	SHOULD		
10.9	If security guards are used, work instructions for security guards are contained in the factory's written policies and procedures. Management must periodically verify compliance and appropriateness with these procedures through audits and policy reviews.	MUST		
11. Personnel Security			*(YES OR NO)*	
11.1	Factory has written processes in place to screen prospective employees and to periodically check current employees. Application information, such as employment history and references, must be verified prior to employment.	MUST		
11.2	Factory performs background checks on all prospective employees in a sensitive position, as well as annually on current employees in sensitive positions. Results of background checks, as permitted by local statutes, should be considered in making hiring decisions.	SHOULD		
11.3	Factory has an Employee Code of Conduct that includes expectations and defines acceptable behaviors. Penalties and disciplinary procedures are included in the Code of Conduct. Employees/contractors acknowledge in writing that they have read and understood the Code of Conduct, and this acknowledgement is kept in the employee's file for documentation.	MUST		
12. Education, Training, and Awareness			*(YES OR NO)*	
12.1	Factory must establish and maintain a security training and awareness program 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. The training program must be comprehensive and cover all of CTPAT's security requirements. Employees in sensitive positions must receive additional specialized training geared toward the responsibilities that the position holds. Factory requires newly hired employees receive security training as part of their orientation/job skills training.	MUST		
12.2	Factory retains evidence of training such as training logs, sign in sheets, or electronic training records. Training records includes the date of the training, names of attendees, and the topics of the training.	MUST		

12.3	Drivers and other employees that conduct security and agricultural inspections of empty containers are properly trained to inspect their containers for both security and agricultural purposes. Security refresher training are conducted periodically, as needed after an incident or security breach, or when there are changes to company procedures.	MUST		
12.4	Factory's inspection training must include the following topics: • Signs of hidden compartments • Concealed contraband in naturally occurring compartments • Signs of pest contamination	MUST		
12.5	Factory should have measures in place to verify that the training provided met all training objectives.	SHOULD		
12.6	Employees are trained on the factory's cybersecurity policies and procedures, which include the need for employees to protect passwords/passphrases and computer access.	MUST		
12.7	Employees operating and managing security technology systems must receive operations and maintenance training in their specific areas.	MUST		
12.8	Employees are trained on how to report security incidents and suspicious activities.	MUST		

Supporting Documentation

Please provide the following documentation to support your responses in each section above:

- **Security Manual -** Copy of factory's security manual addressing how factory maintains each minimum security criterias above
- **Risk Assessment** *(Canada/Mexico only)* - Copy of latest risk assessment
- **Business Parters -** Example of standards and written agreements with carriers, tracking systems, and awareness of CTPAT criteria.
- **Cybersecurity -** Copy of IT training, standards, and disciplinary policy
- **Conveyance and Container Security -** Copy of container inspection procedure and 8-point container checklist
- **Seal Security -** Copy of seal security procedures, copy of seal audit log, photo example of seals used
- **Procedural Security -** Copy of written procedure for incident reporting
- **Agricultural Procedures -** Copy of fumigation certificate
- **Physical Security -** Digital images of key physical structures such as fencing, gates, building structure, electronic surveillance, alarms, etc.
- **Access Controls -** Digital images of employee badges, visitor records/logs, visitor badge, appointments for drivers, etc.
- **Personnel Security -** Copy of employment screening/application, copy of signed employee agreement acknowledging adherance to factory's code of conduct
- **Education, Training and Awareness -** Copy of security awareness training program and training records

CERTIFICATION

I hereby certify that all information provided in connection with this questionnaire is complete, true and accurate in all respects.

Name (Print) ____ Signature ____

Title/Position ____ Date ____