Authorized Economic Operator Security Vetting Items and Validation Criteria

I. Management Organization

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(I) A supply chain security (hereinafter referred to as SCS) management organization must be established to carry out Security and Safety Authorized Economic Operator (hereinafter referred to as AEOS) program.	V	V								
(II) The implementation of AEOS program must be supervised by senior manager.	V	V								
(III) An auditing unit must be established to audit SCS related operation on measures and procedures.	V	V								
(IV) Management organization must fully understand and properly propagandize laws and regulations relevant to SCS.	V	V								

Note: E: Exporter I: Importer M: Manufacturer F: Freight Forwarder
B: Customs Broker W: Warehouse Operator H: Highway Carrier A: Air Carrier
S: Sea Carrier P: Port Terminal Operator

II. Consultation, Cooperation and Communication

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(I) SCS specialists: **At least two staff members who have passed the AEOS SCS training conducted by the Customs or private organization authorized by the Customs must be designated to take charge of the company's SCS operations. What sort of training is held by Customs (content, frequency, costs etc.)? Personal interest in this issue.**	V	V								
(II) Customs communication and consultation window: **Must establish a specific accessible communication window to facilitate communication and consultation with Customs.**	V	V								

III. Physical and Premises Security

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(I) Building structure:										
1. Buildings must be constructed of materials that resist unlawful entry.	V	V	V	V	V	V	V	V	V	V
2. The integrity of structures must be maintained by periodic inspection and repair. The results must be documented.	V	V	V	V	V	V	V	V	V	V

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(II) Proper fencing:										
1. The exterior of Cargo handling area (refer to areas that raw materials, semi-finished goods and finished goods being processed, assembled, and packed) and storage facilities must be surrounded by appropriate fencing.	V	V	V			V				V
2. Interior fencing must be used to segregate raw materials, finished goods, and hazardous items.	V	V	V			V				V
3. All fencing must be maintained by periodic inspection and repair. The results must be documented.	V	V	V			V				V
(III) Segregation of secure areas: **Secure areas must be segregated to facilitate management.**	V	V	V			V				V
(IV) Locking devices and key controls: **All external and internal windows, fences and gates must be secured with locking devices or other security compliance alternatives. Management or security personnel must control the issuance of all locks and keys.**	V	V	V	V	V	V	V	V	V	V
(V) Lighting: **Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas.**	V	V	V	V	V	V	V	V	V	V

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(VI) Alarms and video surveillance systems: **Alarm and video surveillance systems must be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas.**	V	V	V	V	V	V	V	V	V	V
(VII) Security personnel: **Designated employees or the outsourced security company must be responsible for security.**	V	V	V	V	V	V	V	V	V	V

IV. Access Control

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(I) Gate control:										
1. Vehicles/personnel entering or exiting gates must be properly controlled.	V	V	V	V	V	V	V	V	V	V
2. The number of gates should be kept to the minimum necessary for proper access and safety.	V	V	V	V	V	V	V	V	V	V
(II) Personnel access identification system:										
1. Employee identification system:										
(1) An employee identification system must be in place to carry out positive identification and access control.	V	V	V	V	V	V	V	V	V	V

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(2) Employees must only be given access to those secure areas needed for the performance of their duties.	V	V	V	V	V	V	V	V	V	V
(3) The issuance and removal of employee identification badges must be adequately controlled.	V	V	V	V	V	V	V	V	V	V
(4) Procedures for the issuance, removal and changing of access devices (e.g. keys, key cards, etc.) must be documented.	V	V	V	V	V	V	V	V	V	V
2. Visitor identification system:										
(1) Visitors (including suppliers) must present photo identification for documentation purposes upon arrival.	V	V	V	V	V	V	V	V	V	V
(2) All visitors should be escorted and visibly display temporary identification.	V	V	V	V	V	V	V	V	V	V
(3) Proper vendor ID verification mechanism must be in place.	V	V	V	V	V	V	V	V	V	V
(III) Screening mechanism of arriving packages (including mail): Arriving packages and mail must be screened before being disseminated.	V	V	V	V	V	V	V	V	V	V
(IV) Parking: Vehicles must only be parked in designated areas or spaces of secure areas.	V	V	V	V	V	V	V	V	V	V
(V) Suspicious personnel: Procedures must be in place to report unauthorized access and unlawful entry.	V	V	V	V	V	V	V	V	V	V

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(VI) Challenging and removing unauthorized persons: **Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.**	V	V	V	V	V	V	V	V	V	V
(VII) Additional physical access control measures for sea carriers:										
1. Access controls to vessels and cargo facilities:										
(1) Procedures for access controls of employees and visitors must be in place to prevent unauthorized entry to vessels and cargo facilities as well as to protect company assets.									V	
(2) Access controls must include the positive identification of all employees, visitors, service providers, government officials and vendors at all secure access points of entry.									V	
(3) Shore employees and service providers should only have access to those areas of the vessel where they have legitimate business. Vessel and facility access controls are governed by International Ship and Port Security Code (hereinafter referred to as ISPS) and the Maritime Transportation Security Act (hereinafter referred to as MTSA).									V	
2. Controlling vessel boarding and disembarking:										
(1) Consistent with the vessels' ISPS security plan, all crew, employees, vendors and visitors may be subject to a search when boarding or disembarking vessels.									V	

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(2) A vessel visitor log must be maintained and a temporary visitor pass must be issued as required by the vessels' security plan.									V	
(3) All crewmembers, employees, vendors and visitors, including government officials, must display proper identification, as required by the applicable ISPS/MTSA security plan.									V	

V. Employee Security

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(I) Requiring maintaining an employee list: Maintain a current employee list for internal and governmental checks.	V	V	V	V	V	V	V	V	V	V
(II) Requiring pre-employment verification: Application information, such as employment history and references must be verified prior to employment.	V	V	V	V	V	V	V	V	V	V
(III) Conducting background checks/investigations for prospective employees: An appropriate background check/investigation mechanism must be in place for prospective employees according to the sensitivity of specific work items, without violating the basic rights protected by laws and regulations.	V	V	V	V	V	V	V	V	V	V

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(IV) Conducting investigations for current employees: **Companies must conduct periodic investigations for employees with sensitive positions or abnormal social activities or financial status.**	V	V	V	V	V	V	V	V	V	V
(V) Requiring denying access to terminated or transferred employees: **Companies must have procedures in place to remove identification; facility and system access for terminated or transferred employees.**	V	V	V	V	V	V	V	V	V	V

VI. Procedural Security

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(I) Requiring security procedures relevant to cargo transportation, handling, and storage: **Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain.**	V	V	V	V	V	V	V	V	V	V
(II) Requiring information accuracy:										
1. Requiring accurate document processing:										

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(1) Procedures must be in place to ensure that all documentation used in the clearing of cargo, is legible, complete, accurate and protected against the exchange, loss or introduction of erroneous information.	V	V	V	V	V	V	V	V	V	V
(2) Documentation control must include safeguarding computer access and information.	V	V	V	V	V	V	V	V	V	V
2. Requiring accurate and timely manifest procedures: To help ensure the integrity of cargo received from abroad, procedures must be in place to ensure that information received from business partners is reported accurately and timely.		V	V	V	V	V	V	V	V	V
3. Requiring shipping and receiving information against the cargo manifest (bill of lading):										
(1) Import cargo should be reconciled against the information on the bill of lading.		V	V	V	V	V		V	V	V
(2) The weights, labels, marks and piece count of the import/export cargo must be accurately indicated.	V	V	V	V	V	V	V	V	V	V
(3) Import/export cargo must be verified against purchase or delivery orders.	V	V	V	V	V	V	V	V	V	V
(4) Drivers delivering or receiving cargo must be positively identified before cargo is received or released.	V	V	V	V	V	V	V	V	V	V
4. Resolving and reporting cargo discrepancies:										

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(1) All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately.	V	V	V	V	V	V	V	V	V	V
(2) Customs and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected – as appropriate.	V	V	V	V	V	V	V	V	V	V
(III) Requiring additional or written procedural security measures for Customs brokers:										
1. Document processing: **Measures must be in place to ensure that data transmitted by the Customs broker is accurate. Procedures must be in place to ensure that all information provided by the importer/exporter, freight forwarder, etc., and used in the clearing of cargo, is legible and protected against the exchange, loss or introduction of erroneous information.**					V					
2. Ensuring consistent of information: **Ensuring the consistency of information transmitted to Customs through the automatic clearance system with the information that appears on the transaction documents provided to the broker, with regard to such data as the supplier and consignee name and address, commodity description, weight, quantity and unit of measure (i.e. boxes, cartons, etc.) of the cargo being cleared.**					V					

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
3. Ensuring completed/clear documentation: **Review of documentation for completeness and clarity and contracting the business partner or importer/exporter, as necessary, to obtain corrected documentation or information.**					V					
4. Ensuring error-reporting procedures: **To extent such information comes to the broker's attention, alerting the importer/exporter of its obligation to notify Customs and/or shortages and overages of cargo that create a security risk in the supply chain.**					V					
5. Requiring advance cargo information: **Exporters/importers or their agents must submit Customs declaration within the time frame specified by domestic or foreign Customs prior to the cargo arriving at or departing from the port.**					V					
(IV) Requiring additional procedural security measures for sea carriers:										
1. Complying with "Notice of Arrival and Departure" requirements for sea carriers: **Sea carriers much ensure compliance with "Notice of Arrival and Departure" requirements so that accurate, timely and advanced transmission of data associated with international passengers and crew is provided to government agencies and Customs.**									V	

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
2. Providing BAPLIEs on request: **At the request of Customs, sea carriers will provide a requested BAPLIE and/or stowage plan, in a format readily available.**									V	
3. Such requests will be made on a voyage specific basis when Customs requires additional voyage information and will be honored by the sea carrier in a timely manner.									V	

VII. Business Partner Security

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(I) Requiring written procedures for selecting business partners: **Taking supply chain security into consideration, the company must have written and verifiable process for the selection of business partners including Customs brokers, freight forwarders, manufacturers, suppliers, vendors, carriers, port terminal operators, consolidators, and warehouse operators.**	V	V	V	V	V	V	V	V	V	V

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(II) Requiring documentation of partners' AEOS certification: **For those business partners eligible for AEOS certification (carriers, port terminal operators, consolidators, warehouse operators, Customs brokers, freight forwarders, and manufacturers, etc.) the company must have documentation (e.g. photocopy of AEOS certificate) indicating these business partners are certified.**	V	V	V	V	V	V	V	V	V	V
(III) For non-AEOS partners, requiring written confirmation of meeting AEOS-equivalent security criteria:										
1. Requiring business partners without AEOS certificate to provide one of the following written documents demonstrating their compliance with security criteria: **(1) Contractual document.** **(2) A completed self-assessment security questionnaire from the applicant.** **(3) A written statement from the business partner demonstrating their compliance with AEOS security criteria.** **(4) Senior business partner officer attesting to compliance.** **(5) Documents from the business partners demonstrating their compliance with an equivalent and accredited security program administered by a foreign Customs authority.** **(6) A certificate issued by the domestic or foreign third-party security validation institution, which is publicly accepted by the Directorate General of Customs, Ministry of Finance.**	V	V	V	V	V	V	V	V	V	V

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
2. Based upon a documented risk assessment process, non-AEOS eligible business partners must be subject to verification of compliance with AEOS security criteria by the applicant.	V	V	V	V	V	V	V	V	V	V
(IV) Ensuring business partners develop security process and procedures consistent with AEOS security criteria to enhance the integrity of the shipment at point of origin.	V	V	V	V	V	V	V	V	V	V
(V) Periodic reviews of business partners' security condition: Periodic reviews of business partners' processes and facilities should be conducted based on risk, and should maintain the security standards required by the company.	V	V	V	V	V	V	V	V	V	V
(VI) Additional internal partner vetting processes: Requirements such as financial soundness, capability of meeting contractual security requirements, and the ability to identify and correct security deficiencies as needed, should be addressed by the company.	V	V	V	V	V	V	V	V	V	V
(VII) Requiring assessment against a risk-based process as determined by a business partner management team.	V	V	V	V	V	V	V	V	V	V
(VIII) Additional partner vetting processes for air carriers:										
1. Requiring periodic reviews of business partners' security procedures at point of origin.								V		

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
2. AEOS air carriers must ensure business partners develop security processes and procedures consistent with the AEOS security guidelines to enhance the integrity of the shipment at point of origin.								V		
3. Requiring screening and selecting service providers.								V		
4. The AEOS air carrier should have documented service provider screening and selection procedures to screen the contracted service provider for validity, financial soundness, ability to meet contractual security requirements, and the ability to identify and correct security deficiencies as needed.								V		
5. Service provider procedures should utilize a risk-based process as determined by an internal management team.								V		
6. Screening customers:										
(1) The AEOS air carrier should have documented procedures to screen prospective customers for validity, financial soundness, the ability of meeting contractual security requirements, and the ability to identify and correct security deficiencies as needed.								V		
(2) Customer screening procedures should utilize a risk-based process as determined by an internal management team.								V		

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(IX) Additional partner vetting processes for sea carriers:										
1. Requiring written procedures for screening new customers.									V	
2. Sea carriers must have written or web-based procedures for screening new customers to whom they issue bills of lading, which identify specific factors or practices, the presence of which would trigger additional scrutiny by the sea carrier.									V	
3. These procedures must also include a referral to Customs or other competent authorities for further review.									V	
4. The sea carrier must work with Customs to identify specific information regarding what factors, practices or risks are relevant.									V	

VIII. Cargo Security

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(I) Cargo receiving management:										
1. Establishing procedures for the control of cargo receiving:										

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(1) Requiring designated employees in contact with the delivery driver and in charge of cargo receiving.	V	V	V			V				
(2) Requiring registering and verifying shipping documents on cargo and documents required by the Customs.	V	V	V			V				
(3) Requiring recording the completion of inspection and the result.	V	V	V			V				
(4) Requiring active notifying procurement and administration departments of the completion of receiving cargo.	V	V	V			V				
(5) Requiring delivering cargo to the designated areas to prevent the cargo from being unsupervised.	V	V	V			V				
2. Inspecting the seals on cargo delivered: Procedures of inspecting seals must be in place for verifying the intact of the seals when receiving cargo. Routines if the seal are not intact?	V	V	V			V				
3. Designating storage areas with marks: Requiring designated cargo storage areas being clearly marked.	V	V	V			V				
4. Making an inventory or weighing: Standard operation procedures must be in place for making an inventory or weighing of the cargo.	V	V	V			V				
5. Management procedures of cargo receiving:										

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(1) Management procedures of cargo receiving must be in place.	V	V	V			V				
(2) Requiring needed documents, arriving time and designated management personnel for cargo receiving.	V	V	V			V				
(3) Requiring verifying cargo based on purchase order and cargo list.	V	V	V			V				
(4) Requiring completing storage registration right after receiving the cargo.	V	V	V			V				
6. Internal control procedures:										
(1) Internal control procedures must be in place for dealing with anomalies or discrepancies of cargo receiving.	V	V	V			V				
(2) Requiring different departments or personnel being in charge of ordering (procurement), receiving and registering (warehouse management), and payment (disbursement).	V	V	V			V				
(II) Cargo storage management:										
1. Designating cargo storage areas: Requiring designating areas for cargo storage.	V	V	V			V				
2. Internal control procedures:										
(1) Procedures for inventory handling must be in place.	V	V	V			V				

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(2) Procedures for dealing with anomalies or discrepancies must be in place.	V	V	V			V				
3. Separating storage for different cargo:										
(1) Requiring separated storage for different types of cargo (e.g. hazardous cargo, damaged cargo, chemicals etc).	V	V	V			V				
(2) Requiring registering on the logistics management system when the cargo is delivered to the storage area.	V	V	V			V				
4. Additional security measures for receiving cargo: Requiring security measures or additional security methods to protect cargo against access of unauthorized personnel.	V	V	V			V				
5. Authorization level for different type of employees: Requiring only designated staff and authorized personnel are allowed to access storage areas and cargo.	V	V	V			V				
(III) Management of cargo production:										
1. Designating production areas:										
(1) Requiring designating areas for production.			V							

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(2) Requiring security measures and designating management personnel to ensure the integrity and security of cargo if it is outsourced.			V							
2. Internal control procedures:										
(1) Securing production procedures to ensure the integrity and security of cargo in the process of production.			V							
(2) Requiring only designated technicians, authorized personnel or supervisors are allowed to access cargo.			V							
(3) Requiring a system or designated employees to supervise the process of production.			V							
(4) Requiring different departments in charge of manufacturing and production procedures.			V							
3. Additional security measures for access to cargo: Requiring security measures or additional security methods in the process of production to protect cargo from the access of unauthorized personnel.			V							
4. Employee authorization level and classification: Requiring only designated technicians and authorized personnel are allowed to access cargo.			V							
5. Quality inspection: Quality inspection procedures must be in place to further ensure the security and integrity of cargo.			V							

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(IV) Loading management:										
1. Routine check of cargo:										
(1) Requiring designated personnel in contact with the delivery driver and in charge of cargo loading.	V		V			V				
(2) Requiring registering and verifying the shipping documents on cargo and the documents required by the Customs.	V		V			V				
(3) Requiring verifying cargo, shipping documents on cargo and the documents required by the Customs.	V		V			V				
(4) Requiring recording the completion of inspection and the result.	V		V			V				
(5) Sales and administration department must be actively notified of the cargo status as it is shipped from the company.	V		V			V				
2. Loading supervision: **Requiring designating personnel in charge of supervising the loading of cargo.**	V		V			V				
3. Consistent marking: **Requiring cargo to be shipped must be consistently marked and stored in designated areas.**	V		V			V				

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
4. Weighing cargo with record: **Operation procedures must be in place for making an inventory and weighing cargo with record.**	V		V			V				
5. Management process of cargo loading and delivery:										
(1) Requiring needed documents, time and management personnel for cargo loading, and they must be consistent with shipping record of warehouse management.	V		V			V				
(2) Requiring verifying cargo based on shipping list.	V		V			V				
(3) Requiring completing the shipping registration as the cargo is shipped from the company and must be consistent with the shipping record of warehouse management.	V		V			V				
6. Sealing of the cargo to be shipped: **Requiring verifying and sealing export cargo to be shipped in accordance with Customs regulations.**	V		V			V	V		V	
7. Internal control procedures: **Internal control procedures must be in place for dealing with anomalies or discrepancies of cargo to be shipped.**	V		V	V	V	V	V		V	
(V) Management of cargo to be exported:										

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
1. Security measures must be in place for export cargo delivered by trucks, bonded trucks, bonded cartons, or containers to export warehouses, terminal operators, or export ports to protect against loss, theft, or damage.										
(1) The seals for containerized export cargo must meet or exceed the current ISO PAS 17712 standards (e.g. electronic seal) for high security seals.	V		V	V			V		V	
(2) Requiring using seals issued or authorized by Customs for export cargo shipped by bonded trucks or bonded cartons.	V		V	V			V		V	
(3) Proper security measures for export cargo delivered by truck must be in place to ensure cargo security.	V		V							
2. Requiring drivers to check the integrity of seals and record the result before delivering export cargo.	V		V			V	V			
(VI) Maintaining logistics data: Ensuring the integrity and correctness of the content of the documents/electronic data of cargo transaction, logistics, and Customs clearance with a mechanism to protect against tampering, exchange, or loss.	V	V	V	V	V	V	V	V	V	
(VII) Additional container security requirements for warehouses:										

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
1. Requiring complying with relevant regulations governing Customs management of warehouses (e.g. warehouses, bonded warehouses, logistics centers, terminal operators, etc.)						V				
2. Standard operation procedures must be in place for controlling the storage, withdrawal, and transfer of container/cargo.						V				
3. Security measures for cargo storage areas must be in place to protect against the access of unauthorized personnel.						V				
4. Adequate measures must be in place to protect against unauthorized movement, exchange, or damage.						V				

IX. Container Security

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(I) Requiring secure container storage: Containers must be stored in a secure area to prevent unauthorized access and/or manipulation.	V	V	V	V		V	V		V	V
(II) Requiring container integrity at point of stuffing:										

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
1. Container integrity must be maintained to protect against the introduction of unauthorized material and/or persons.	V	V	V	V		V	V		V	V
2. At the point of stuffing, procedures must be in place to properly seal and maintain the integrity of the shipping containers.	V	V	V	V		V	V		V	V
(III) Transmission of container/cargo movement message: Requiring relevant business of import, export, transit and transshipment transmitting container information to the Dynamic Tracking System of Containers (Cargoes) in accordance with "Operational Directions for the Dynamic Tracking System of Containers (Cargoes)".	V	V	V	V		V			V	V
(IV) Container security:										
1. Procedures must be 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.	V		V			V	V		V	V
2. A seven-point inspection process is required for loaded containers.										
(1) Inside/outside doors	V		V			V	V		V	V
(2) Front wall	V		V			V	V		V	V
(3) Left side	V		V			V	V		V	V
(4) Right side	V		V			V	V		V	V

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(5) Floor	V		V			V	V		V	V
(6) Ceiling/Roof	V		V			V	V		V	V
(7) Outside/undercarriage	V		V			V	V		V	V
(V) Requiring ISO PAS 17712 standard high security seals: All seal must meet or exceed the current ISO PAS 17712 standards for high security seals.	V	V	V	V		V	V		V	V
(VI) Controlling container seals:										
1. Written procedures must stipulate how seals are to be controlled and affixed to loaded containers.	V	V	V	V		V	V		V	V
2. Procedures must be in place for recognizing and reporting compromised seals and/or containers to Customs.	V	V	V	V		V	V		V	V
3. Requiring designated units or employees to distribute container seals and record the use of seals for integrity purposes.	V	V	V	V		V	V		V	V
(VII) Management of empty containers: Requiring a mechanism (including designated areas, periodic patrol, etc.) to protect against unauthorized access.	V	V	V			V	V	V	V	V

X. Conveyance Security

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(I) Requiring maintaining management procedures for security of conveyance (e.g. trucks, vessels, aircrafts etc.):										
1. Procedures must be in place for preventing unauthorized entry into conveyance to ensure conveyance security.	V	V	V			V	V	V	V	
2. Security measures for conveyance:										
(1) Requiring periodic search of internal/external cargo hold for suspicious persons or goods.	V	V	V			V	V	V	V	
(2) Securing all internal/external compartments, or walls/doors of vessels and aircraft.								V	V	
(3) Procedures must be in place to address unauthorized entry or other illegal cases.	V	V	V			V	V	V	V	V
(4) Procedures must be in place to address unmanifested goods in vessels or aircraft.						V		V	V	V
3. Routes for receiving and delivering cargo must be predetermined.	V	V	V			V	V			
4. Ensuring confidentiality of the cargo to be loaded and the planned routes and destinations.	V	V	V			V	V			
5. Management procedures must be in place for keys, parking areas, fueling, and unplanned stops.	V	V	V			V	V			
6. Procedures must be in place for reporting incidents or emergencies.	V	V	V			V	V	V	V	

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
7. Procedures must be in place for reporting anomalies of cargo or seals.	V	V	V			V	V	V	V	
(II) Additional security requirements for air carriers:										
1. Requiring procedures for maintaining aircraft integrity.								V		
2. Aircraft integrity must be maintained to protect against the introduction of unauthorized personnel and material.								V		
3. Conveyance security procedures must include the physical search of all readily accessible areas, securing all internal/external compartments and panels and reporting cases in which unmanifested materials or signs of tampering are discovered.								V		
(III) Requiring additional security measures for highway carriers, or documentation of compliance with AEOS security criteria:										
1. Requiring conveyance tracking and monitoring procedures:										
(1) En route conveyance security: Highway carriers must ensure that conveyance and trailer integrity is maintained while the conveyance is en route transporting cargo to export/import points or import/transit containers by utilizing a tracking and monitoring activity log or records.							V			

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(2) Predetermined routes and random security checks: **Predetermined routes must be identified by the dispatcher, and procedures must consist of random route checks along with documenting and verifying the length of time between the loading point/trailer pickup and the delivery destinations.**							V			
(3) Notification of route delays: **Drivers should notify the dispatcher of any route delays due to weather, traffic and/or rerouting.**							V			
(4) Periodic, unannounced and documented checks by carrier management: **Highway carrier management must perform a documented, periodic, and unannounced verification process to ensure the logs are maintained and conveyance tracking and monitoring procedures are being followed and enforced.**							V			
2. Conveyance inspection procedures:							V			
(1) Using a checklist for conveyances inspection: **Using a checklist, drivers should be trained to inspect their conveyances for security.**							V			
(2) Training in conveyance searches: **Training in conveyance searches should be adopted as part of the company's on-the-job training program.**							V			

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(3) Inspecting conveyance upon both entering and exiting truck yard: **Conveyance inspections must be completed upon entering and departing from the truck yard and at the last point of loading prior to export and/or import.**							V			
(4) Random search by security managers: **To counter internal conspiracies, supervisory personnel or a security manager, held accountable to senior management for security, must search the conveyance after the driver has conducted a search.**							V			
(5) Searches must be random, documented, and based on risk.							V			
(6) Searches must be conducted at the truck yard and after the truck has been loaded and en route to import and/or export.							V			
(IV) Requiring additional security measures for bonded trucks, or documentation of compliance with AEOS security criteria:										
1. Requiring loading/unloading vigilance: **Highway carriers must be vigilant to help ensure that the merchandise is legitimate and that there is no loading of contraband at the loading lock/manufacturing facility.**							V			

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
2. Requiring secure bonded trucks storage: **Bonded trucks must be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting unauthorized entry into or storage in correct areas.**							V			
3. Requiring bounded truck seals:										
(1) Based on risk, a high security barrier bolt seal must be applied to the door handle and/or a cable seal must be applied to the vertical bar on the bonded truck doors.							V			
(2) All seal must meet or exceed the current ISO PAS 17712 standards for high security seals.							V			
4. Requiring procedures for treatment of goods in transit:										
(1) Clearly defined written procedures must stipulate how seals in the highway carrier's possession are to be controlled during transit.							V			
(2) These written procedures must be briefed to all drivers.							V			
(3) There must be a mechanism to ensure that these procedures are understood and are being followed.							V			
5. Requiring procedures for treatment of goods in transit include:										
(1) Verifying that the seal is intact, and if it exhibits evidence of tampering along the route.							V			

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(2) Verify that the seal number is the same as stated on the shipping documents.							V			
(3) Properly documenting the original and second seal numbers.							V			
(4) The driver must immediately notify the dispatcher that the seal was broken, by whom; and the number of the second seal that is placed on the bonded truck.							V			
(5) The carrier must immediately notify the relevant partners or authorities of the placement of the second seal.							V			
(V) Additional security requirements for port terminal operators:										
1. Requiring protecting conveyance against tampering.										V
2. Conveyance/vessel integrity must be maintained to protect against the introduction of unauthorized personnel and material.										V
3. Conveyance/vessel security procedures must include the physical search of all readily accessible areas, securing all internal/external compartments, panels and reporting cases in which unmanifested materials or signs of tampering are discovered.										V
4. Requiring full collaboration with other business entities at ports for inspection and transmission of real-time trade data, container (cargo) status and high-risk targets.										V

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
5. While at port, the pier and waterside of vessel must be adequately illuminated. Limit shore employees and service providers to those areas of the vessel where they have legitimate business.										V
6. Requiring constant contact with CSI local representatives to discuss supply chain security issues with further improvement in which the international port is deployed with CSI representatives.										V

XI. Information Technology Security

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(I) Information security management:										
1. Proper procedures of information security management must be in place to protect information system against unauthorized access or misuse.	V	V	V	V	V	V	V	V	V	V
2. Automated systems can only be accessed with individually assigned accounts, and they must be protected with passwords that must be changed periodically.	V	V	V	V	V	V	V	V	V	V
3. IT security policies, procedures and standards must be in place and provided to employees in the form of annual training.	V	V	V	V	V	V	V	V	V	V
(II) Requiring IT accountability:										

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
1. A system must be in place to identify the abuse of IT including improper access, tampering or the altering of business data.	V	V	V	V	V	V	V	V	V	V
2. All system violators must be subject to appropriate disciplinary actions for abuse.	V	V	V	V	V	V	V	V	V	V
(III) Information classification and control:										
1. Requiring mechanisms for proper classifying and managing information (including documents) based on its sensitivity and priority.	V	V	V	V	V	V	V	V	V	V
2. Requiring proper securing or encrypting for critical and sensitive information with periodic audit based on the condition of its use.	V	V	V	V	V	V	V	V	V	V
(IV) Information backup and recovery: Data backup and recovery procedures must be in place to protect against information loss.	V	V	V	V	V	V	V	V	V	V

XII. Security Training and Threat Awareness

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(I) Establishing a threat awareness program:										

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
1. A threat awareness program should be established and maintained to recognize and foster awareness of the threat at each point in the supply chain.	V	V	V	V	V	V	V	V	V	V
2. Employees must be made aware of the procedures the company has in place to address a situation and how to report it.	V	V	V	V	V	V	V	V	V	V
3. Additional training should be provided to employees in the shipping and receiving areas, as well as those receiving and opening mail.	V	V	V			V				V
(II) Developing supply chain security training for employees: Specific training should be offered to assist employees in maintaining cargo integrity, recognizing internal conspiracies, and protecting access controls.	V	V	V	V	V	V	V	V	V	V
(III) Supply chain security training of employees must include the following items:										
1. Security policy of the company.	V	V	V	V	V	V	V	V	V	V
2. Potential risk to internal security of the company.	V	V	V	V	V	V	V	V	V	V
3. Maintaining cargo security.	V	V	V	V	V	V	V	V	V	V
4. Access control measures of the company.	V	V	V	V	V	V	V	V	V	V
5. Identifying and reporting suspicious cargo and personnel.	V	V	V	V	V	V	V	V	V	V

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(IV) Keeping records of security training: **Requiring keeping records of security training for the checks conducted by the Customs.**	V	V	V	V	V	V	V	V	V	V
(V) These programs must offer incentives for active employee participation.	V	V	V	V	V	V	V	V	V	V
(VI) Conveyance management personnel must receive training in conveyance maintenance and cargo security.	V	V	V			V	V	V	V	V
(VII) Additional security awareness requirements for sea carriers:										
1. Identifying and reporting security protocol shortcomings.									V	
2. Carriers and Customs have a mutual interest in security assessments and improvements, and recognize that specific, implemented security, procedures may be found in the future to have weaknesses or be subject to circumvention. When a security shortcoming or security incident is identified, the carrier and Customs officials will meet in an effort to ascertain what led to the breakdown and to formulate mutually agreed remedial measures.									V	
3. If Customs determines that the security incident raises substantial impact or a security weakness requires substantial remediation, Customs headquarters officials will meet with the carrier's senior management to discuss such concerns and to identify appropriate remedial measures to be taken.									V	

XIII. Incident Prevention and Handling

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(I) Incident reporting: **All shortages, overages, anomalies of loading/unloading and other violations of security management must be reported to Customs and internal units.**	V	V	V	V	V	V	V	V	V	V
(II) Mechanism of risk management: **The mechanism of risk management must be in place to deal with serious incidents or emergencies.**	V	V	V	V	V	V	V	V	V	V
(III) Incident drill:										
1. Periodic incident drill and test must be held.	V	V	V	V	V	V	V	V	V	V
2. The mechanism of the drill must be updated when the internal operation or organization alters.	V	V	V	V	V	V	V	V	V	V
(IV) Incident investigation procedures and analysis: **Investigation procedures must be in place for the occurred incidents to identify the causes and revise the mechanism of incident prevention and handling to protect against the recurrence.**	V	V	V	V	V	V	V	V	V	V

XIV. Assessment and Improvement

Validation Criteria	E	I	Business Partner							
			M	F	B	W	H	A	S	P
(I) Security assessment:										
1. Requiring conducting self-assessment annually based on the security criteria announced by the Customs.	V	V	V	V	V	V	V	V	V	V
2. Requiring conducting periodic risk assessment regarding the company's operation in supply chain security and establishing the appropriate mechanism to reduce risk.	V	V	V	V	V	V	V	V	V	V
(II) Keeping records of security assessment: **Requiring designated personnel in charge of security assessment and relevant complete documentation.**	V	V	V	V	V	V	V	V	V	V
(III) Continuous security management: **Requiring a security management mechanism in accordance with assessment results and recommendations for possible enhancements to be incorporated in a plan for the forthcoming period to ensure its continuity and soundness.**	V	V	V	V	V	V	V	V	V	V