ANNEXURE 1			
AEO Criteria Structure Applicable to Self-Assessment Questionnaire (SAQ)			
Criteria	**Sub Criteria**		**Explanatory Notes**
A. Demonstrated Compliance with Customs Requirements	**A.1**	Record of Any Infringements/Offences	This criterion requires the applicant to demonstrate a satisfactory level of compliance with national Customs-related laws and to have an effective system in place for quality assurance of Customs declarations. The criteria are to be fulfilled by the applicant, or by designated persons. Customs takes into account the totality of the facts, along with mitigating and aggravating factors (deliberate offence, repeated offences, financial gain, etc.) in its decision to determine if the applicant is qualified to become an AEO. Examples of serious infringements are: • Smuggling; • Fraud, for example, deliberate misclassification, undervaluation and overvaluation, or false declaration of origin to avoid payment of Customs duties; • Infringements related to Intellectual Property Rights (IPR); • Infringements related to prohibited and restricted goods; • Facilitating or involvement in fraudulent activities; • Any other offence related to Customs requirements; • Bankruptcy (insolvency) fraud; • Any infringement of health or environmental legislation; • Participation in a criminal organization; • Bribery and corruption; • Cybercrime; • Money laundering, etc.; • Direct or indirect involvement in terrorist activities. Applicants should be able to demonstrate the effectiveness of their systems and procedures for meeting such requirements.
	A.2	Tax and Customs Duty Payment	Applicants should provide detailed statements on any overdue or unpaid taxes or Customs duties with Customs, and verify the appropriate channel or contact point to address any arrears in Customs duties/Tax.

	A.3	Quality Assurance of Customs Declarations	Applicants should provide the list of goods they trade in that are subject to economic trade licences/restrictions, and provide the relevant licence/permit or approval from competent authorities. Applicants should be able to describe their procedures for administering the licences/ permits for the import and/or export of such goods. Applicants must describe their quality assurance procedures for verifying the accuracy of Customs declarations, including those submitted on their behalf by service providers such as Customs brokers/ clearing agents.
B. Satisfactory System for Management of Commercial Records	**B.1**	Commercial Records Management Framework	It is important for a company to have a well-written, adopted, and implemented set of policies and procedures. Policies and procedures encourage consistency in how one manages records. They specify what information an organization must keep in the form of records, the procedures for managing those records, retention issues, data security, maintenance and secure disposal. In addition, the manual/guidelines may address items such as business processes and workflow, and the role of records management within them. Guidelines and procedures are designed to help the company and its employees meet their record-keeping obligations and to foster good practice. It is recommended that policies comply with relevant legislative and statutory requirements and international standards. In this context, the company should provide Customs with access to necessary records and make available any authorizations, powers of attorney and licences relevant to the importation or exportation of goods, subject to the requirements of national legislation. It is important that companies have an effective commercial records management system, as well as accounting system in place. However, these systems should provide Customs with insights into the flow of goods and money, as well as the tax aspects, related to import and export. It is also critical that the systems be well equipped and structured to securely capture, store/archive, process, manage, retrieve and protect

			data/information and permit Customs to conduct necessary audits in order to fulfil required mandates and obligations effectively. Further, the system needs to ensure quality data/information and provide timely, accurate, complete and verifiable import and export records with clear procedures outlined. In particular, for Customs purposes, the system should take into account the following: • Proper archiving of records for later presenting to Customs, within any limitations provided under national legislation. • Employment of adequate information technology security measures which will protect against access by unauthorized persons. • Proper procedures laid out for back-up, recovery, fall-back, archiving and retrieval of business records. Audit trails are the manual or electronic records that chronologically catalogue events/transactions or procedures, providing proper documentation and history that are used to authenticate security and operational actions, or mitigate challenges. Internal control has four basic purposes: safeguarding assets, ensuring financial statement reliability, promoting operational efficiency, and encouraging compliance with the management's directives. Good internal controls are essential to ensuring the accomplishment of goals and objective, provide reliable financial reporting for management decisions and ensure compliance with applicable laws and regulations to avoid unnecessary risk and problems. A company should have a good procedure with adequate checks and balances, in line with its overall policy framework. That procedure should take into account and encompass all the possible risks. These include the detection, identification and reporting of incorrect, incomplete and/or out-of-date information and transactions which are being maintained and recorded in the system (e.g. tariff classifications, taxes, commodity details) for Customs purposes.
	B.2	Commercial Records Management System	

	B.3	Internal Control System	
C. Financial Viability	**C.1**	Proven Financial Standing	Financial viability means good financial standing which is sufficient to fulfil the commitments of the applicant (i.e. the entity is to be able to pay all its debts as and when they become due and payable), with due regard to the characteristics of the type of business activity and current economic conditions. Financial statements based on national generally accepted accounting principles serve as an objective basis on which to determine the financial standing of a company. Where the company is required by national law to have its financial statements audited by an external auditor, these should be provided. The applicant should disclose whether the company is or has been the subject of bankruptcy or bankruptcy protection proceedings, and details of the bankruptcy proceedings should be disclosed. A record of accurate and timely payments to Customs of duties, taxes and fees can serve as evidence of a good compliance record and
	C.2	Bankruptcy Proceedings	
	C.3	Obligations	

			commitment to meeting Customs obligations over a period of time, reinforcing trust.
D. Consultation, Cooperation and Communication	**D.1**	Exchange of Information	Customs-to-Business Partnerships require contact points to be established for both parties, with a mechanism to engage both parties in an open and continued mutual exchange of information, where legally acceptable. Transparency in communication is key to building trust and encouraging meaningful exchange of information. For example, business can make use of information available on Customs' website, distributing it to its employees and others in the supply chain. Documented procedures should outline how shortages, overages, and other significant cargo discrepancies or anomalies are investigated and resolved, as appropriate. Likewise, procedures should be in place to promote the efficient and secure flow of information to Customs and law enforcement authorities when security incidents occur or anomalies are detected as well as any incident involving an emergency or disaster. This is to include a description of the facility's escalation process (who is notified first, what and when information is documented, etc.). Notification procedures must include complete and accurate contact information that lists the name(s), phone number(s) and email addresses, if available, of Customs personnel, as well as other law enforcement agencies, as appropriate. Procedures must be periodically reviewed to ensure contact information is accurate.
	D.2	Discrepancy Reports for Goods and Items	
	D.3	Emergency Reporting and Contingency Planning	

E. Education, Training and Threat Awareness	**E.1**	Internal Trade Security Training System	The applicant is required to have mechanisms in place for educating and training personnel regarding security policies and regarding recognition of deviations from those policies. There should be a clear understanding of what actions must be taken in response to security lapses. Relevant training may relate to the security measures, procedures and policies an applicant has in place to ensure the integrity of the international supply chain. Employees who are aware of security risks and threats, their company's role in the supply chain, and understand why security measures are in place, are more likely to adhere to such measures. Security education ensures that employees receive the training required to identify, prevent and respond to security threats and breaches. Employees must be provided with trade security training on a regular basis, and at least once a year. Newly-hired employees must receive this training as part of their orientation/job skills training. Contractors must also be provided with security training, based on the job being performed. The training programme must be comprehensive and cover all AEO security requirements. Drivers and other personnel that conduct security inspection of empty conveyances and Instruments of International Traffic (IIT) must be trained to inspect their conveyances/IIT for security purpose. As applicable, based on their functions and/or positions, personnel must be trained on the company's cybersecurity policies and procedures. This must include the need for employees to protect passwords/passphrases and computer access. Personnel operating and managing security technology systems must receive operations and maintenance training in their specific areas. Prior experience with similar systems is acceptable. Self-training via operational manuals and other methods is acceptable. Additional training topics may include protecting access controls, recognizing internal conspiracies, and reporting procedures for suspicious activities and security incidents. Members must retain evidence of training, such as training logs, sign-in sheets (rosters), or electronic training records. Training records should include the

			date of the training, names of attendees, and the topics of the training. Quality training is important to lessen vulnerability to cyberattacks. A robust cybersecurity training programme is usually one that is delivered to applicable personnel in a formal setting, rather than simply through emails or memos. The prevalence of smuggling schemes that involve the modification of conveyances or IIT makes it imperative that drivers conduct inspections of conveyances and IIT to look for serious structural deficiencies.

	E.2	Education and Training on the Risks Associated with the Flow of Goods and Articles in the International Trade Supply Chain	It is important for AEO companies to establish and maintain a trade security training and awareness programme in order to recognize and foster awareness of the security vulnerabilities of facilities, conveyances and cargo at each point in the supply chain, which could be exploited by terrorists or contraband smugglers. Security training and awareness is not a one-time exercise. Regular security training through various methods is ideal. Routine company-wide updates help ensure security concerns are current and remain "top-of-mind" throughout your organization. In addition to a record of training completed by employees, companies should have measures in place to verify that the training provided has met all training objectives. Understanding the training and being able to use that training in one's position (for sensitive employees) is of paramount importance. Exams or quizzes, simulation exercises/drills, or regular audits of procedures, etc. are some of the measures that the company may implement to determine the effectiveness of the training.
	E.3	Crisis Management Training and Crisis Management Simulation Exercises	A crisis may include the disruption of the movement of trade data due to a cyberattack, a fire, or a carrier driver being hijacked by armed individuals. Based on risk and where the member operates or sources from, contingency plans may include additional security notifications or support, and how to recover what has been destroyed or stolen, with a view to returning to normal operating conditions. Personnel must be trained on how to report security incidents, suspicious activities, and emergencies. Procedures to report security incidents, suspicious activities, and emergencies are extremely important aspects of a security programme. Specialized training modules (based on job duties) may provide more detailed training on reporting procedures, including specifics such as what to report and to whom, how to report an incident, and what to do after the report is completed.

	E.4	Internal Training System on Customs Laws and Regulations	A company's compliance with Customs laws and regulations is an essential component of AEO programme eligibility and continued authorization. Specialized training on Customs laws and regulations must be provided to personnel involved in processes within the Customs purview (e.g. import/export documentation, and movement of goods across the border). Training should be specific and relevant to the employee's job responsibilities in complying with Customs laws and regulations (e.g. reporting requirements on imports, or a transport driver's compliance regarding personal effects when crossing the border) and must be conducted annually so that the employee stays abreast of evolving and emerging schemes.
F. Information Exchange, Access and Confidentiality	**F.1**	Import/Export Activities	Import/export management procedures should be comprehensive, to effectively control the flow of cargo, documentation and information. There should be written procedures for all import/export activities in order to control movements of goods, to ensure that employees are following the same processes, and to prevent errors. This should include a process methodology or flow chart.

	F.2	Data Security	Members must have comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems. These policies and procedures must be reviewed annually – or more frequently, as risk or circumstances dictate. Following the review, policies and procedures must be updated if necessary. The written IT policy, as a minimum, must address what the company has done in order to: • Defend IT systems against common cybersecurity threats. To this end, a company must install sufficient software/hardware protection against malware (viruses, spyware, worms, Trojans, etc.) and against internal/external intrusion (firewalls) in Members' computer systems. • Ensure that its security software is current and receives regular security updates and prevent attacks via social engineering. • Recover (or replace) IT systems and/or data should a data breach occur or another unforeseen event result in the loss of data and/or equipment. • Regularly test the security of its IT infrastructure if using network systems. If vulnerabilities are found, corrective actions must be implemented as soon as feasible. Individuals with access to information technology (IT) systems must use individually assigned accounts. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication, and user access to IT systems must be safeguarded. Passwords and/or passphrases must be changed as soon as possible if there is evidence of compromise or reasonable suspicion that a compromise exists. A system must be in place to identify unauthorized access to IT systems/data or abuse of policies and procedures, including improper access to internal systems or external websites, and tampering or altering of business data by employees or contractors. There should be a policy for controlling access to the IT server room or access list. Only authorized personnel should have access to the server room. Procedures should be in place to address the need to back up data. Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format. Media

			used to store back-ups should preferably be stored at a facility off-site. Quality training is important to lessen vulnerability to cyberattacks. A robust cybersecurity training programme is usually one that is delivered to applicable personnel in a formal setting, rather than simply through emails or memos. As applicable, based on their functions and/or positions, personnel must be trained on the company's cybersecurity policies and procedures. This must include the need for employees to protect passwords/passphrases and computer access. All company personnel that violate the IT cybersecurity policies must be subject to appropriate disciplinary action, which may include termination of employment.

G. Cargo Security	**G.1**	Safety Management System of Cargo	Security measures should be in place to ensure that the integrity of cargo is maintained, and that irregular practices relevant to the flow of goods (transportation, handling and storage of cargo) in the international supply chain are prevented. It is important to have 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. Personnel need to review the information included in import/export documents to identify or recognize suspicious cargo shipments. Relevant personnel need to be trained on how to identify information in shipping documents, such as manifests, that might indicate a suspicious shipment. If paper documents are used, forms and other import/export-related documentation should be secured to prevent unauthorized use.
	G.2	Loading and Receipt of Cargo	Arriving cargo should be reconciled against information on the cargo manifest. All shortages, overages, and other significant discrepancies or anomalies need to be investigated and resolved, as appropriate. Information transmitted to Customs should be consistent with the information that appears on the transaction documents provided to the broker. This information includes the supplier and consignee name and address, commodity description, weight, quantity, and unit of measure (boxes, cartons, etc.) of the cargo being cleared. Sound internal controls dictate that only authorized individuals be allowed to sign company forms and documents, and that procedures governing such authority be in writing and properly disseminated to all affected employees. In addition, controls over seals should be documented, and all concerned personnel should be trained and supervised to ensure compliance with seal security policies and procedures. Documented evidence of the properly installed seal (for example, digital photographs) should be taken at the point of stuffing. To the extent feasible, these images should be electronically forwarded to the destination for verification purposes.

	G.3	Export Security	Procedures need to be 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. Personnel need to review the information included in import/export documents to identify or recognize suspicious cargo shipments. Relevant personnel must be trained on how to identify information in shipping documents, such as manifests, that might indicate a suspicious shipment. If paper documents are used, forms and other import/export-related documentation should be secured to prevent unauthorized use. Departing cargo should be verified against purchase or delivery orders. Based on risk, management personnel should conduct random searches of containers and conveyances after the transportation staff have conducted conveyance/IIT inspections. The searches of the conveyance should be done periodically, with a higher frequency based on risk. The searches should be conducted at random and without warning, so that they do not become predictable. The inspections should be conducted at various locations and times where the conveyance is susceptible: the carrier yard, after the truck has been loaded, and en route to an international border or point of exportation. Documented evidence of the properly installed seal (for example, digital photographs) should be taken at the point of stuffing. To the extent feasible, these images should be electronically forwarded to the destination for verification purposes. The completed 7-point/8-point container inspection sheet (see below) should be part of the shipping documentation packet. The consignee should receive the complete shipping documentation packet prior to receiving the merchandise.

	G.4	Container Safety Management System	The prevalence of smuggling schemes that involve the modification of conveyances or IIT makes it imperative that AEO members have written procedures in place outlining how they inspect and document the inspections of conveyances and IIT to ensure the integrity and security of the container/IIT. The inspection process needs to outline written procedures for security inspection purpose. Written procedures must include and describe: How the company ensures that systematic security inspections are being conducted. A 7-point inspection must be conducted on all empty containers and unit load devices (ULDs); and an 8-point inspection must be conducted on all empty refrigerated containers and ULDs: 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. Fan housing (if refrigerated container). The written procedures must also include and describe: How containers are stored in a secure area to prevent unauthorized access, which could result in an alteration to the structure, or (as applicable) allow the seal/doors to be compromised. How conveyances and IIT (such as containers/ULDs) are equipped with external hardware that can reasonably withstand attempts to remove it. 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. The inspection of all conveyances and empty IIT must be recorded on a checklist. The following elements should be documented on the checklist: • Container/trailer/IIT number • Date of inspection • Time of inspection • Name of employee conducting the inspection, and • Specific areas of the IIT that were inspected. If the inspections are supervised, the supervisor

			should also sign the checklist. The completed container inspection sheet should be part of the shipping documentation packet. The consignee should receive the complete shipping documentation packet prior to receiving the merchandise.
	G.5	Container Inspection	As part of the overall seal audit process, dock supervisors and/or warehouse managers must periodically verify seal numbers used on conveyances and IIT. These 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.

	G.6	Container Seals	Detailed, written high-security seal procedures that describe how seals are issued and controlled at the facility and during transit are critically important. Procedures need to address the steps to take if a seal is altered/tampered with, or if a document has the incorrect seal number. They also need to address communication protocols to partners, and the investigation of the incident. The findings from the investigation should be documented, and any corrective actions must be implemented as quickly as possible. If an AEO member maintains an inventory of seals, company management or a security supervisor must conduct a periodic seal audit that includes taking an inventory of stored seals and reconciliation against seal inventory logs and shipping documents. All audits must be documented. The sealing of trailers and containers to attain continuous seal integrity continues to be a crucial element of a secure supply chain. Seal security includes having a comprehensive written seal policy that addresses all aspects of seal security, such as using the correct seals, per AEO requirements: a high-security seal that meets or exceeds the most current International Standardization Organization (ISO) 17712 standard for high-security seals.
	G.7	Container Storage	Conveyances and IIT must be stored in a secure area to prevent unauthorized access, which could result in an alteration to the structure of an Instrument of International Traffic, or (as applicable) allow the seal/doors to be compromised. Procedures must be in place to identify, challenge and address unauthorized/unidentified persons. Personnel must know the protocol for challenging an unknown/unauthorized person, how to respond to the situation, and be familiar with the procedure for removing an unauthorized individual from the premises. Members must have written procedures for reporting an incident, which includes a description of the facility's internal escalation process. Procedures must be periodically reviewed to ensure contact information is accurate.

	G.8	Driver Identity Verification	Drivers delivering or receiving cargo need to be positively identified before cargo is received or released. Where operationally feasible, AEO members should allow deliveries and pick-ups by appointment only. This is designed to help shippers and carriers avoid fictitious pick-ups. Fictitious pick-ups are criminal schemes that result in the theft of cargo by deception. If GPS technology is employed, geo-fencing must be implemented and is to include alarm notification when a carrier deviates from the assigned route. The parameters for geo-fencing must be set at minimal allowable tolerances for the pre-established transit route.
H. Conveyance Security	**H.1**	Security Management System for Conveyance	Documented measures should be in place to ensure the integrity of cargo during its conveyance (transportation, handling and storage of cargo) in the international supply chain. Based on risk, If a GPS tracking system is used, carriers should use a sensor coupling/connector or equivalent technology from the tractor to the trailer to ensure the trailer is also monitored and tracked. Shippers should have access to their carrier's GPS fleet monitoring system so that they may track the movement of their shipments. If driver logs are used, the driver must record any stops and note that inspections were made of the conveyance, Instrument of International Traffic (IIT), and the security seal.

	H.2	Conveyance Inspection	It is critically important that conveyances be inspected so that they are not carrying any illegal or undeclared items. Prior to stuffing/packing, all empty IIT need to be inspected, and conveyances must also be inspected if they cross international land borders. For trucks, these systematic inspections must include: Tractors: 1. Bumper/tyres/rims 2. Doors, tool compartments and locking mechanisms 3. Battery box 4. Air breather 5. Fuel tanks 6. Interior cab compartments/sleeper 7. Fairing/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 mechanisms 10. Outside/undercarriage. It is good practice, based on risk, for management personnel to conduct random searches of conveyances after the transportation staff have conducted conveyance/IIT inspections. at various locations and times where the conveyance is susceptible, such as the carrier yard, or after the truck has been loaded. The inspection of all conveyances should be recorded on a checklist. As a minimum, the following elements should be documented on the checklist: • Date of inspection • Time of inspection • Name of employee conducting the inspection • Specific areas of the conveyance inspected. After a stop, drivers should inspect the conveyance's sealing or locking devices for any signs of tampering prior to resuming the trip. These inspections should be documented. Drivers and other personnel that conduct security inspection of empty conveyances and IIT must be trained to inspect their conveyances/IIT for security purposes

			so that they may understand the threats to the supply chain and what they need to do to mitigate/eliminate those threats. Refresher training must be conducted periodically, as needed after an incident or security breach, or when there are changes to company procedures. Inspection training must include the following topics: • Signs of hidden compartments • Concealed contraband in naturally occurring compartments. AEO members must have written procedures for reporting a credible suspicion or an incident, which includes a description of the facility's internal escalation process. Notification procedures need to include accurate contact information that lists the name(s) and phone number(s) of personnel requiring notification, as well as for law enforcement agencies. AEOs should periodically review these procedures to ensure contact information is accurate. Examples of incidents warranting notification include: • Discovery of tampering with a container/IIT or high-security seal; • Discovery of a hidden compartment in a conveyance or IIT; • An unaccounted new seal has been applied to an IIT; • Smuggling of contraband, including people; stowaways; • Unauthorized entry into conveyances, locomotives, vessels, or aircraft carriers; • Extortion, payments for protection, threats and/or intimidation.

	H.3	Conveyance Storage	All cargo handling and storage facilities, including trailer yards and offices, should have physical barriers and/or deterrents that prevent unauthorized access. Private passenger vehicles should be prohibited from parking in, or adjacent to, cargo handling and storage areas and conveyances. Locate parking areas outside fenced and/or operational areas – or at least, at substantial distances from cargo handling and storage areas. If a credible (or detected) threat to the security of a shipment or conveyance is discovered, the AEO member must alert (as soon as feasibly possible) any business partners in the supply chain that may be affected, and any law enforcement agencies, as appropriate.
	H.4	Transport Process Control	Companies must have written procedures to protect the integrity of shipping data related to the transport units, such as seal numbers, driver names and their company ID, transport unit's licence plate and/or unit number, unit weight, etc. Transporters may want to track and monitor their conveyances in real time. Based on risk, If a GPS tracking system is used, carriers should use a sensor coupling/connector or equivalent technology from the tractor to the trailer to ensure the trailer is also monitored and tracked.
I. Premises Security	**I.1**	Safety and Security Management System of Premises	This criterion requires applicants to have physical security measures in place, in addition, security measures should be in place to prevent unauthorized access to offices, shipping areas, loading docks, cargo areas and other relevant places, in order to secure access to the premises and to prevent tampering with goods. It is critical for companies to have written procedures to ensure systematic security inspections are conducted throughout the company's premises. A documented periodic inspection should be conducted of all high-risk areas, such as entry/exit gates, building windows, doors, alarm devices, perimeter fencing, exterior lighting, and video surveillance equipment to ensure that structures are adequately protected against unauthorized access or activities, and that any security breaches are detected and reported in a timely manner.

	I.2	Exit/Entry	Gates where vehicles and/or personnel enter or exit (as well as other points of egress, such as entrances to facilities that are not gated) must be manned or monitored. It is recommended that the number of gates be kept to the minimum necessary for proper access and safety.
	I.3	Building Structures	Preventing unauthorized access to business premises, including offices, warehouse and packing facilities (not agricultural fields), is critical to ensure that company information, conveyances and cargo are not tampered with or stolen. AEO companies need to ensure that these premises have physical barriers and/or deterrents that prevent unauthorized access. Barriers and deterrents (to include fencing, walls, doors, windows, etc.) should be regularly inspected for integrity by designated personnel. If damage is found, repairs should be made as soon as possible. Every building, plant or facility needs to be inspected regularly as part of an overall maintenance programme. Ideally, inspections are scheduled, completed on time, and documented with a report of findings. A competent person should conduct the inspection and the AEO company should take prompt corrective measures to eliminate any hazardous conditions or security gaps. This inspection should include all exterior doors, walls, and widows; exterior lighting; fences, and gates.
	I.4	Lighting	Adequate lighting is an important security feature – 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. Automatic timers or light sensors that automatically turn on appropriate security lights are useful additions to lighting apparatus.

	I.5	Video Surveillance	Electronic security technology used to secure/monitor sensitive areas and access points includes: burglary alarm systems (perimeter and interior), also known as Intrusion Detection Systems (IDS); access control devices; and video surveillance systems (VSS), including Closed Circuit Television (CCTV) cameras. A CCTV/VSS system could include components such as analogue cameras (coax-based), Internet Protocol (IP)-based cameras (network-based), recording devices, and video management software. Secure/sensitive areas which would benefit from video surveillance may include: building entry and reception areas, cargo handling and storage areas, shipping/receiving areas where import documents are kept, IT servers, rooms where IT servers are stored, yard and storage areas for containers, areas where containers are inspected, and seal storage areas.
	I.6	Warehousing Area	All business structures (offices, warehouses, packing facilities, etc.) must have physical barriers and/or deterrents that prevent unauthorized access. Agricultural fields do not need to comply with these requirements but, based on risk, may want to adopt other security safeguards, such as security patrols.
	I.7	Locking Devices and Key Custody	Based on risk, internal and external windows and doors should be equipped with locking devices. Members need to have written procedures governing how access devices, such as keys, are granted, changed, and removed. Removal of access devices must take place when the employees separate from the company.
	I.8	Access Control Management System	It is recommended that the number of gates be kept to the minimum necessary for proper access and safety. Other points of egress would be entrances to facilities that are not gated.

	I.9	Employee Access Control	Generally, for a company with more than 50 employees, an identification system is required. There is need to need to have written procedures governing how identification badges and access devices are granted, changed, and removed. Access devices include employee identification badges, visitor and vendor temporary badges, biometric identification systems, proximity key cards, codes and keys which should be retrieved when employees separate from the company. Access to sensitive areas must be restricted, based on job description or assigned duties. Private passenger vehicles should be prohibited from parking in, or adjacent to, cargo handling and storage areas and conveyances.
	I.10	Visitor Access Control	Written processes should be in place and effectively implemented, and are to include the following: Visitors, vendors and service providers must present photo identification upon arrival, and a log must be maintained that records the details of the visit. All visitors should be escorted. In addition, all visitors and service providers should be issued with temporary identification. If temporary identification is used, it must be visibly displayed at all times during the visit. The registration log must include the following: • Date of the visit, and visitor's name; • Verification of photo identification (type verified, such as licence 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; and • Time of departure.
	I.11	Control of Unauthorized Access and Unidentified Persons	Procedures need to be in place to identify, challenge and address unauthorized/unidentified persons. It is very important for personnel to know the protocol for challenging an unknown/unauthorized person, how to respond to the situation, and to be familiar with the procedure for removing an unauthorized individual from the premises.

J. Personnel Security	**J.1**	Personnel Security Management System	The criterion requires reasonable precautions to be taken when recruiting staff, in order to verify that they have not previously been convicted of security-related Customs or other offences. Employee background screening should include verification of the employee's identity and criminal history, and draw on city, state, provincial, and country databases.
	J.2	Employee File Management	The company should have accurate and updated records of its employees, which list, among other things, the names of the employees/contractors; position titles; departments they work for; entry dates and, if applicable, departure date.
	J.3	Pre-Employment Review	Prospective employees should be properly identified with some type of government-issued photo identification (driver's licence, passport, national identification card, etc.).
	J.4	Employee Separation Management	Written procedures should outline the company's personnel suspension and termination processes, to include the removal of access devices (keys, badges, etc.) when the employees separate from the company. Companies should consider other items that could be used to compromise access, such as uniforms. The use of exit checklists is recommended to ensure that all access devices have been returned and/or deactivated. Businesses that allow their users to connect remotely to a network should employ secure technologies, such as virtual private networks (VPNs), to allow employees to securely access the company's intranet when located outside the office. Members should also have procedures to secure against remote access by unauthorized users
	J.5	Visitor Identification and Registration	Visitors, vendors and service providers must present photo identification upon arrival, and a log must be maintained that records the details of the visit. All visitors and service providers should be issued with temporary identification badges and should be escorted by a company representative throughout the facility, including to such areas as kitchenettes and restrooms.
	J.6	Identification and Disposition of Unauthorized Access and Unidentified Persons	Personnel must be trained on how to identify, challenge and respond to the situation, and be familiar with the procedure for removing an unauthorized individual from the premises.

			Personnel must also be trained on how to report all security incidents (such as unauthorized entry and unauthorized persons).
K. Trading Partner Security	**K.1**	Business Partner Security Control System	This criterion requires measures to be in place that business partners ensure the security of their part of the international supply chain. AEO companies need to have a written, risk-based process for screening new business partners and for monitoring current partners. AEOs need to have procedures in place that outline how they can clearly identify their business partners, and to ensure (through implementation of appropriate contractual arrangements, security declarations or other appropriate measures in accordance with the AEO company's business model) that those business partners also do their due diligence to secure the international supply chain. The following are examples of some of the vetting elements that can help determine if a company is legitimate: • Verifying the company's business address and how long they have been at that address; • Conducting research on the internet on both the company and its principals; • Checking business references; and • Requesting a credit report. Examples of business partners that need to be screened are direct business partners, such as manufacturers, product suppliers, pertinent vendors/service providers, and transportation/logistics providers. Any vendors/service providers that are directly related to the company's supply chain and/or handle sensitive information/equipment are also to be included on the list to be screened; this includes Customs brokers or contracted IT providers.

	K.2	Comprehensive Assessment	The business partner screening process can take into account whether a partner is a member of an approved Authorized Economic Operator (AEO) programme with a Mutual Recognition Agreement/Arrangement (MRA) with the member where AEO status was granted. It can also take into account whether the business partner is certified by a recognized security organization that conducts supply chain security audits on its own members, and based on AEO standards. Specific procedures should be in place for identifying regular business partners and unknown companies, including procedures to select subcontractors based on a risk-assessed list of regular and irregular subcontractors. Subcontractors In cases where a business partner hires subcontractors to perform any services required under the agreement between companies and the business partner, the companies should be aware of the number of steps of subcontractors that the business partner hires. This should be stated in the agreement. In addition, International Chamber of Commerce (ICC) Incoterms used in buyer/seller transactions can be taken into account when assessing business partners, as additional evidence of business arrangements when assessing the security risks of business trading partners.
	K.3	Written Documents	A business partner's certification in an approved AEO programme, or by another recognized security organization, is acceptable proof that the business partner meets programme requirements. Companies must obtain evidence of the certification and continue to monitor these business partners to ensure they maintain their certification. Companies that outsource or contract out elements of their supply chain should exercise due diligence (via visits, questionnaires, etc.) to ensure business partners have security measures in place that meet or exceed the AEO requirements. Determining if a business partner is compliant with the AEO requirements can be accomplished in several ways. Based on risk, the company may conduct an on-site audit at the facility, hire a contractor/service provider to conduct an on-site audit, or use a security questionnaire.

	K.4	Regular Checks	To ensure their business partners continue to comply with all applicable AEO programme requirements, companies should update their security assessments of their business partners on a regular basis, or as circumstances/risks dictate, and at least annually. Deciding on how often to review a partner's security assessment is based on the company's risk assessment process. Higher-risk supply chains would be expected to have more frequent reviews than low-risk ones. Circumstances that may require the self-assessment to be updated more frequently include an increased threat level from a source country, changes in source location, or new critical business partners (those that actually handle the cargo, provide security to a facility, etc.).
L. Crisis Management and Incident Recovery	**L.1**	Contingency Plan	An applicant should have a crisis management, recovery and security plan in order to minimize the impact of a disaster or security incident. Companies should have written procedures in place that address crisis management, business continuity, security recovery plans, and business resumption. A crisis or emergency may include the disruption of the movement of trade data due to a cyberattack, a fire, or a carrier driver being hijacked by armed individuals. Based on risk and where the member operates or sources from, contingency plans may include additional security notifications or support; and how to recover what was destroyed or stolen, in order to return to normal operating conditions. Contingency plans need to be updated, based on risks and lessons learned.
M. Measurement, Analyses and Improvement	**M.1**	Internal Audit/Review Mechanism on Import/Export Activities	The applicant is required to establish and conduct regular self-assessments of its security management system, and fully document the self-assessment procedure and the responsible parties. The goal of an internal audit/review is to ensure that employees are following the company's procedures. The company decides the scope of the audit/review and how in-depth it should be – based on its role in the supply chain, business model, level of risk, and variations between specific locations/sites. The internal audit/review

			activities are usually conducted by company employees.
	M.2	Monitoring Activities	The internal audit/review activities need to be performed regularly, i.e. once a year. A member may choose to use smaller targeted reviews directed at specific procedures. Specialized areas that are key to supply chain security, such as inspections and seal controls, may undergo reviews specific to those areas. However, it is useful to conduct an overall general review periodically to ensure that all areas of the security programme are working as designed. For members with high-risk supply chains (determined by their risk assessment), simulation or table top exercises may be included in the audit to ensure personnel will know how to react in the event of a real security incident.
	M.3	Internal Audit to Assess Continuous Compliance with AEO Criteria	The role of internal audit is to provide independent assurance that a company's risk management, governance and internal control processes are operating effectively. A review process of AEO requirements may be included in the context of internal control of the company.

	M.4	Corrective Measures	If weaknesses are identified during business partners' security assessments, they must be addressed as soon as possible, and corrections must be implemented in a timely manner. Companies must confirm via documentary evidence that deficiencies have been mitigated. Based on the level of risk involved and the importance of the weakness found, some issues may require immediate attention. If it is a deficiency that may jeopardize the security of a container, for instance, it should be addressed as soon as possible. Examples of documentary evidence may include copies of contracts for additional security guards, photographs taken of a newly installed security camera or intrusion alarm, or copies of inspection checklists, etc.