



REQUIREMENTS RESPECTING THE SECURITY OF OFFSHORE FACILITIES

Definitions

1. In these requirements:

“C-NLOPB” means the Canada-Newfoundland and Labrador Offshore Petroleum Board;

“Chief Safety Officer” means the Chief Safety Officer of the C-NLOPB;

“declaration of security” means an agreement between any of the following that specifies the security procedures that each will implement when interfacing with one another:
a vessel;
a marine facility; and
an offshore facility.

“ISPS Code” means the International Ship and Port Facility Security Code, as incorporated into SOLAS;

“MARSEC level 1” means the level for which minimum protective security procedures are maintained at all times;

“MARSEC level 2” means the level for which protective security procedures additional to those of MARSEC level 1 are maintained for a period as a result of heightened risk of a security incident;

“MARSEC level 3” means the level for which protective security procedures additional to those of MARSEC level 1 and MARSEC level 2 are maintained for a limited period when a security incident is probable or imminent regardless of whether the specific target is identified;

“offshore facility” means a marine facility in a maritime zone of Canada as described in Part I of the *Oceans Act*, and includes a drilling unit or platform;

“security incident” means any suspicious act or circumstance that threatens the security of a vessel, marine facility or an offshore facility or an interface between any of them; and

“SOLAS” means International Convention for the Safety of Life at Sea, 1974, as amended.

Operator of an Offshore Facility

2. The operator of an offshore facility shall ensure that the requirements of this Part are met.
3. The operator of an offshore facility shall:
 - (a) establish an administrative and organizational structure for security at the offshore facility;
 - (b) provide every person that has responsibilities under these requirements with the support needed to meet their responsibilities;
 - (c) designate in writing, by name, a company security officer and an offshore facility security officer;
 - (d) operate the offshore facility in compliance with the offshore facility security plan and any temporary measures referred to in paragraph 6(*h*);
 - (e) when the offshore facility is interfacing with a marine facility, operate the offshore facility in compliance with the marine facility security plan;
 - (f) report any significant security threat, breach of security or security incident to the Chief Safety Officer; and,
 - (g) ensure that the implementation of security procedures is coordinated with vessels and marine facilities with which the offshore facility interfaces and, where applicable, with port administrations.

Company Security Officer

4. (1) A company security officer may:
 - (a) act in that capacity for more than one offshore facility if:
 - (i) the company security officer is able to meet the responsibilities for each of the

- offshore facilities, and,
 - (ii) Each of the offshore facility plans lists the other offshore facilities;
 - (b) have other responsibilities within the organization of the operator of the offshore facility if they are able to perform the responsibilities of the company security officer;
 - (c) delegate tasks required by these requirements; and,
 - (d) act as an offshore facility security officer if another person who is shoreside and within the organization is designated to ensure effective communication with competent authorities and to coordinate changes in the MARSEC levels or response to security incidents.
 - (2) A company security officer remains responsible for the performance of the tasks they delegate.
5. (1) The company security officer shall have, by training or job experience, knowledge or competence in the areas that relate to the position at the offshore facility for which they have been designated.
- (2) The areas of knowledge and competence shall include the following:
 - (a) the administration and structure of security for the offshore facility;
 - (b) the operations and conditions of the offshore facility;
 - (c) the security procedures of the offshore facility including the meaning and requirement of the different MARSEC levels;
 - (d) emergency preparedness and response and contingency planning;
 - (e) security equipment and systems and their operational limitations;
 - (f) methods of conducting audits and inspections and control and monitoring techniques;
 - (g) techniques for security training and education, including security regulations, measures, rules and procedures;
 - (h) relevant international conventions, codes, standards and recommendations;
 - (i) relevant legislation, regulations and security measures, rules and procedures;
 - (j) the responsibilities and functions of municipal, provincial and federal law enforcement agencies;
 - (k) methods of conducting offshore facility security assessments;
 - (l) methods of handling sensitive security information and security-related communications;
 - (m) current security threats and patterns;
 - (n) the detection and recognition of weapons, explosives, incendiaries and other dangerous substances and devices;
 - (o) the recognition of the characteristics and behavioral patterns of persons who are likely to threaten security;
 - (p) techniques that might be used to violate security procedures or to circumvent security procedures, equipment or systems;
 - (q) methods of conducting physical searches and non-intrusive inspections; and,
 - (r) conducting and assessing security drills and exercises.
6. A company security officer shall:
 - (a) keep the offshore facility manager or offshore facility security officer informed of threats and other information relevant to its security;
 - (b) enhance security awareness and vigilance in the organization of the operator of the offshore facility;
 - (c) submit offshore facility security assessment information to the Chief Safety Officer;
 - (d) submit an offshore facility security plan, as well as any amendment, to the Chief Safety Officer for approval;
 - (e) ensure that the offshore facility security plan and any amendment to it are implemented;
 - (f) ensure that the security activities of the offshore facility are audited;
 - (g) as soon as practicable after a deficiency in the offshore facility security plan is identified, amend it as required to correct the deficiency;
 - (h) ensure that temporary measures are implemented to correct a deficiency referred to in paragraph (g) until such time as the offshore facility security plan is amended;
 - (i) provide a copy of the offshore facility security assessment to the offshore facility security officer;
 - (j) provide a copy of the offshore facility security plan to the offshore facility security officer;
 - (k) maintain a record of the names and responsibilities of all offshore facility personnel that have security responsibilities, including information on how they may be contacted at any time;
 - (l) ensure that there is consistency between the security requirements and safety requirements;
 - (m) ensure that security procedures take into account the convenience, comfort and personal privacy of offshore facility personnel and their ability to maintain their effectiveness over long periods of time;

- (n) ensure that personnel receive adequate security training as required by these requirements; and,
- (o) ensure that there is effective communication and cooperation between the offshore facility and interfacing vessels.

Offshore Facility Security Officer

7. (1) An offshore facility security officer may:
 - (a) act in that capacity for more than one offshore facility if:
 - (i) the offshore facilities are within reasonable proximity to each other,
 - (ii) the offshore facility security officer is able to meet their responsibilities for each offshore facility, and,
 - (iii) each of the offshore facility security plans lists the other offshore facilities for which the officer is responsible;
 - (b) have other responsibilities in the offshore facility operator's organization if they are able to fulfill the responsibilities of the offshore facility security officer; and,
 - (c) delegate tasks required by these requirements to other offshore facility personnel.
 - (2) An offshore facility security officer remains responsible for the performance of the tasks that they delegate.
8. (1) An offshore facility security officer shall have, by training or job experience, knowledge in the areas that relate to their position at the offshore facility for which they have been designated.
 - (2) The areas of knowledge include the following:
 - (a) those set out for a company security officer in subsection 5(2);
 - (b) the physical layout of the offshore facility;
 - (c) the offshore facility security plan and its requirements; and,
 - (d) the operation, testing and maintenance of security equipment and systems.
9. An offshore facility security officer shall:
 - (a) regularly inspect the offshore facility to ensure compliance with these requirements;
 - (b) prepare the offshore facility security assessment information referred to in section 20 and submit it to the company security officer;
 - (c) prepare an offshore facility security plan based on the offshore facility security assessment and submit it to the company security officer;
 - (d) implement and maintain the offshore facility security plan;
 - (e) conduct audits of the offshore facility security plan and procedures as specified by these requirements;
 - (f) as soon as practicable after a deficiency in the offshore facility security plan is identified, report it to the company security officer and implement the corrective action that is required to correct the deficiency;
 - (g) propose amendments to the offshore facility security plan to the company security officer to correct any deficiencies;
 - (h) ensure security awareness and vigilance at the offshore facility, including awareness of changes in MARSEC levels and other circumstances that might affect the work conditions at the offshore facility;
 - (i) ensure that adequate security training is provided to personnel at the offshore facility as required by these requirements;
 - (j) report security threats and security incidents to the company security officer, appropriate law enforcement agencies and the Chief Safety Officer as soon as possible after they occur and conduct an investigation into them;
 - (k) ensure that security equipment is operated, tested, calibrated and maintained in compliance with the offshore facility security plan;
 - (l) ensure consistency between security requirements and the proper treatment of offshore facility personnel affected by those requirements;
 - (m) when a change in the MARSEC level is implemented, record and report this to the company security officer, the operator of the offshore facility and the Chief Safety Officer; and,
 - (n) keep a copy of the offshore facility security assessment and plan readily accessible.
10. (1) Persons who have responsibilities respecting the security of an offshore facility other than the company security officer or offshore facility security officer shall have, by training or job experience, knowledge in the areas that relate to their position at the offshore facility.
 - (2) The areas of knowledge include the following:
 - (a) current security threats and patterns;

- (b) the detection and recognition of weapons, explosives, incendiaries and other dangerous substances and devices;
 - (c) the recognition of the characteristics and behavioral patterns of persons who are likely to threaten security;
 - (d) techniques that might be used to violate security procedures or to circumvent security procedures, equipment or systems;
 - (e) crowd management and control techniques;
 - (f) security-related communications;
 - (g) emergency preparedness and response and contingency planning;
 - (h) the operation, testing, calibration and maintenance of security equipment and systems;
 - (i) Inspection, control and monitoring techniques of the offshore facility;
 - (j) methods of performing physical searches of persons and goods including personal effects, baggage, ships' stores and industrial supplies;
 - (k) the relevant provisions of the offshore facility security plan; and,
 - (l) the meaning and requirements of the different MARSEC levels.
11. A person who is assigned to an offshore facility and who does not have security responsibilities shall receive security training or security orientation in:
- (a) basic security issues and communications;
 - (b) the meaning of the different MARSEC levels, the different procedures required of the person at each level and the emergency procedures and contingency plans;
 - (c) the detection and recognition of weapons, explosives and incendiaries and other dangerous substances and devices;
 - (d) the recognition of the characteristics and behavioral patterns of persons who are likely to threaten security; and,
 - (e) techniques that might be used to violate security procedures or to circumvent security procedures, equipment or systems.

Security Drill and Exercise Requirements

12. Security drills and exercises shall test the proficiency of offshore facility personnel in assigned security responsibilities at all MARSEC levels and the effective implementation of the offshore facility security plan and shall enable the offshore facility security officer to identify any related security deficiencies that need to be corrected.
13. (1) The offshore facility security officer shall ensure that a security drill is conducted:
- (a) at least once every three months; or,
 - (b) as soon as practicable after operations resume at an offshore facility that has been out of service or inactive for more than three months.
- (2) A security drill may be conducted with drills that are not related to security.
- (3) Security drills shall test individual elements of the offshore facility security plan including response to security threats, breaches of security and security incidents and shall take into account, in respect of the offshore facility, the types of operations, personnel changes, the types of vessels interfacing with it and other relevant circumstances.
- (4) If, at any given time, more than 25% of the permanent personnel at the offshore facility have not participated in a security drill within the previous three months, a security drill shall be conducted within one week.
- (5) If an offshore facility is involved in the implementation of MARSEC level 2 or MARSEC level 3 following a security incident, the implementation of the MARSEC level shall be equivalent to a drill.
14. (1) Security exercises:
- (a) shall fully test the offshore facility security plan and include the substantial and active participation of personnel who have security responsibilities;
 - (b) may include security personnel from vessels, marine facilities, other offshore facilities or competent authorities depending on the scope and the nature of the exercises;
 - (c) may be performed with respect to only the offshore facility or as part of a cooperative program to test another offshore facility security plan or a vessel, marine facility or port administration security plan; and,
 - (d) shall test communication and notification procedures and elements of coordination, resource availability and response.
- (2) The exercises shall be conducted at least once every calendar year with no more than 18 months between them.

- (3) Exercises may be:
 - (a) full-scale or live;
 - (b) tabletop simulation or seminar;
 - (c) combined with other appropriate exercises; or,
 - (d) a combination of the elements set out in paragraphs (a) to (c).

Record Keeping

15. (1) An offshore facility security officer shall keep records of:
 - (a) security training, including the date, duration and description and the names of the participants;
 - (b) security drills and exercises, including the date and description, the names of the participants and any best practices or lessons learned that might improve the offshore facility security plan;
 - (c) security threats, breaches of security and security incidents, including the date, time, location, description and response and the identity of the person to whom it was reported;
 - (d) changes in the MARSEC level, including the date, the time that notification was received and the time of compliance with the security requirements of the new level;
 - (e) maintenance, calibration and testing of equipment used in security, including the date and time of the activity and the specific equipment involved;
 - (f) Declarations of security signed in respect of the offshore facility;
 - (g) internal audits and reviews of security activities;
 - (h) each periodic review of the offshore facility security assessment, including the date on which it was conducted and the findings of the review;
 - (i) each periodic review of the offshore facility security plan, including the date on which it was conducted, the findings of the review and any amendments to the offshore facility security plan that are recommended;
 - (j) each amendment to the offshore facility security plan, including the date of approval and implementation; and,
 - (k) a list of the names of the persons who have security responsibilities.
- (2) Records respecting equipment that is not used exclusively for security may be kept separately from records respecting equipment that is used exclusively for security if:
 - (a) the offshore facility security officer documents, in written or electronic form, their existence and location and the name of the person responsible for their maintenance; and,
 - (b) they are accessible by the offshore facility security officer.
- (3) The offshore facility security officer shall ensure that the records are kept for at least two years after they are made and make them available to the Chief Safety Officer on request.
- (4) The records shall be protected from unauthorized access or disclosure.
- (5) The records may be kept in electronic format if they are protected from deletion, destruction and revision.

Communications

16. (1) The offshore facility security officer shall have the means to notify the offshore facility personnel of changes in security conditions at the offshore facility.
- (2) The offshore facility shall have communication systems and procedures that allow effective communications
 - (a) between the offshore facility security personnel and vessels, marine facilities and other offshore facilities interfacing with it; and,
 - (b) the Chief Safety Officer and local law enforcement agencies.
- (3) Communications systems shall have a backup to ensure internal and external communications.

Declarations of Security

17. (1) A declaration of security signed in respect of an offshore facility shall address the security requirements that are shared between the offshore facility and a vessel, marine facility or other offshore facility with which it is interfacing, state the responsibilities of each and be completed and signed before the interface starts.
- (2) The declaration of security shall:
 - (a) be in English or French;

- (b) contain the information set out in the form in Appendix 1 of Part B of the ISPS Code, with the terms “ship”, “port facility” and “security measures” substituted by “vessel”, “offshore facility” and “security procedures” respectively;
 - (c) be completed and signed by
 - (i) the manager of the offshore facility or the offshore facility security officer, or,
 - (ii) any person who has security responsibilities and appropriate training and has been designated in writing by either person set out in subparagraph (i) to complete a declaration of security on their behalf;
 - (d) in the case of another facility, be completed if there is an interface with a vessel, marine facility or other offshore facility that:
 - (i) is operating at a lower MARSEC level than that of the offshore facility,
 - (ii) is not required to have a security plan, or,
 - (iii) Has experienced a security threat, breach of security or security incident; and,
 - (e) in the case of another facility, be completed if there is an interface with a marine facility.
- (3) A new declaration of security shall be completed if there is a change in MARSEC levels.
 - (4) Except in the case of a facility at MARSEC level 1 if the facility interfaces with a vessel or other offshore facility that is carrying certain dangerous cargo in bulk or is to be loaded with certain dangerous cargo in bulk, the offshore facility security officer shall complete and sign a declaration of security.
 - (5) The offshore facility security officer shall complete and sign a declaration of security if they identify an interface that is of special concern.
 - (6) Except in the case of a facility at MARSEC level 1 and MARSEC level 2 the offshore facility security officer may implement a continuing declaration of security for a vessel with which the offshore facility frequently interfaces if the effective period does not exceed:
 - (a) 90 days for MARSEC level 1; and,
 - (b) 30 days for MARSEC level 2.

Offshore Facility Security Assessments

- 18. (1) Security assessment information in respect of an offshore facility:
 - (a) shall be in writing and in either English or French;
 - (b) shall be based on the collection of background information, the completion of an on-site survey and an analysis of that information and survey;
 - (c) shall contain:
 - (i) an identification and evaluation of the physical aspects of the offshore facility that are the most important to protect and the means for protecting the personnel,
 - (ii) an identification of possible threats to the offshore facility, and the likelihood of their occurrence, in order to establish and security procedures and countermeasures and their order of priority, and,
 - (iii) identification of the weaknesses, including human factors, in the security of the offshore facility;
 - (d) may cover more than one offshore facility if they are contiguous; and,
 - (e) shall be protected from unauthorized access or disclosure.
 - (2) The offshore facility security assessment information shall be submitted to the Chief Safety Officer for the assessment to be conducted.
 - (3) The offshore facility security plan shall not be submitted before the approval of a completed offshore facility security assessment by the Chief Safety Officer.
- 19. The persons who provide security assessment information shall have, collectively, the competence to evaluate the security of the offshore facility including knowledge in the following areas:
 - (a) current security threats and patterns;
 - (b) the detection and recognition of weapons, explosives and incendiaries and other dangerous substances and devices;
 - (c) the recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
 - (d) techniques that might be used to violate security procedures or to circumvent security procedures, equipment or systems;
 - (e) methods used to cause a security incident;
 - (f) the effects of dangerous substances and devices on structures and essential services;
 - (g) offshore facility security requirements and, if applicable, port administration security requirements;
 - (h) offshore facility and vessel and marine facility interface business practices;

- (i) emergency preparedness and response and contingency planning;
 - (j) physical security requirements;
 - (k) radio and telecommunications systems, including computer systems and networks;
 - (l) marine or civil engineering; and,
 - (m) offshore facility and vessel operations.
20. (1) Security assessment information shall consist of the following:
- (a) the general layout of the offshore facility, including the location of:
 - (i) active and inactive access points to the offshore facility,
 - (ii) security doors, barriers, and lighting,
 - (iii) restricted areas,
 - (iv) emergency and stand-by equipment available to maintain essential services,
 - (v) maintenance equipment, storage areas and unaccompanied baggage storage,
 - (vi) escape and evacuation routes and assembly stations, and,
 - (vii) existing security and safety equipment for protection of personnel and visitors;
 - (b) changes in the tide that may have an impact on the vulnerability or security of the offshore facility;
 - (c) a list of the emergency and stand-by equipment available to maintain essential services;
 - (d) the number of offshore facility personnel, the security tasks of persons with security responsibilities and the training requirements and procedures of the offshore facility;
 - (e) existing security and safety equipment for the protection of offshore facility personnel and visitors;
 - (f) escape and evacuation routes and assembly stations that have to be maintained to ensure the orderly and safe emergency evacuation of the offshore facility;
 - (g) the results of security audits; and,
 - (h) security procedures in effect, including inspection and control procedures, identification systems, surveillance and monitoring equipment, personnel identification documents and communication, alarms, lighting, access control and other appropriate systems.
21. An offshore facility security assessment shall address the following elements in respect of the offshore facility, as applicable:
- (a) the physical security;
 - (b) the structural integrity;
 - (c) personnel protection systems;
 - (d) operational procedures that may impact on security;
 - (e) the radio and telecommunication systems including computer systems and networks;
 - (f) relevant transportation support infrastructure;
 - (g) utilities; and,
 - (h) other elements that might, if damaged or used illicitly, pose a risk to people, property or operations at the offshore facility.
22. An offshore facility security assessment shall take into account all likely threats, including, but not limited to, the following types of security incidents:
- (a) damage to, or destruction of, the offshore facility, a vessel or a marine facility by explosive devices, arson, sabotage or vandalism;
 - (b) tampering with essential equipment, systems or stores of the offshore facility;
 - (c) unauthorized access;
 - (d) the smuggling of weapons or equipment, including weapons of mass destruction;
 - (e) use of the offshore facility itself as a weapon or as a means to cause damage or destruction;
 - (f) nuclear, biological, radiological, explosive and chemical attacks on the shoreside support system of the offshore facility or a vessel or marine facility interfacing with it;
 - (g) the seizure of the offshore facility or the seizure or hijacking of a vessel or marine facility interfacing with the offshore facility or seizure of a person in any of them; and,
 - (h) use of the offshore facility to carry those intending to cause a security incident or their equipment.

On-scene Survey and Vulnerability Assessments

23. The operator of an offshore facility shall ensure that an on-scene survey of the offshore facility is conducted. The survey shall examine and evaluate current protective procedures and operations to verify or collect the information referred to in section 20.
24. (1) An offshore facility security assessment shall include a vulnerability assessment undertaken in consultation with the operator of the offshore facility to determine the following so as to

produce an overall assessment of the level of risk against which security procedures have to be developed:

- (a) whether any particular aspect of the offshore facility, including vessel traffic in the vicinity, would make it a likely target of an attack;
 - (b) the possible consequences of an attack on or at the offshore facility in terms of loss of life, damage to property and economic disruption, including the disruption of transport systems;
 - (c) the capability and intent of those likely to mount an attack; and,
 - (d) the possible type of attack.
- (2) The vulnerability assessment shall include a consideration of the following:
- (a) current security procedures, including identification systems;
 - (b) methods and points of access to the offshore facility;
 - (c) the procedures to protect radio and telecommunication equipment, including computer systems and networks;
 - (d) any conflicting policies between safety and security procedures;
 - (e) any enforcement or personnel constraints;
 - (f) methods for monitoring restricted areas and other areas that have restricted access to ensure that only authorized persons have access;
 - (g) areas adjacent to the offshore facility that might be exploited during or for an attack;
 - (h) current security procedures relating to utilities and other services;
 - (i) any deficiencies identified during training or drills;
 - (j) any deficiencies identified during daily operations or following incidents or alerts, reports of security concerns, the exercise of control measures or audits; and,
 - (k) the structural integrity of the offshore facility.

Offshore Facility Security Plan

25. An offshore facility security officer shall establish an offshore facility security plan for each of the offshore facilities for which they are responsible.
26. An offshore facility security plan:
- (a) shall be in writing and in English or French;
 - (b) shall be protected from unauthorized access or disclosure;
 - (c) shall, if stored in electronic format, have procedures to prevent its unauthorized deletion, destruction or amendment;
 - (d) shall be submitted to the Chief Safety Officer for approval;
 - (e) is valid for a period determined by the Chief Safety Officer which shall not exceed five years after the date of the Chief Safety Officer's approval; and,
 - (f) may cover more than one offshore facility if they share similarities in physical characteristics, location and operations.
27. An offshore facility plan shall be based on the findings of the offshore facility security assessment, address each vulnerability identified in the assessment and include:
- (a) the organization of the offshore facility in terms of security, including the tasks of personnel who have security responsibilities;
 - (b) the name and title of the operator, company security officer and offshore facility security officer, including information on how they may be contacted at any time;
 - (c) the identification of restricted areas, and any security procedures, equipment and systems for restricted areas;
 - (d) a description of procedures and frequency of drills and exercises;
 - (e) a description of procedures for the following:
 - (i) ensuring the security of information in the offshore facility security plan and keeping the records referred to in section 15,
 - (ii) maintaining security and communication systems and equipment,
 - (iii) identifying and responding to equipment or systems failure or malfunction,
 - (iv) communications,
 - (v) Response to changes in the MARSEC level,
 - (vi) interfacing with vessels or marine facilities at each MARSEC level,
 - (vii) declarations of security,
 - (viii) preventing unauthorized weapons, explosives, incendiaries or other dangerous substances or devices from entering the offshore facility,
 - (ix) reporting security threats, breaches of security and security incidents to the competent authorities,
 - (x) Securing non-critical operations in order to focus response on critical operations,

- (xi) the periodic review, updating and audits of the offshore facility security plan; and,
 - (f) a description of
 - (i) security procedures, equipment and systems for access control,
 - (ii) security procedures for the delivery of ships' stores and industrial supplies,
 - (iii) security procedures, equipment and systems for monitoring the offshore facility and surrounding area, and,
 - (iv) security threat, breach of security and security incident procedures including procedures for the evacuation of the offshore facility.
28. (1) An offshore facility security plan shall contain security procedures at each MARSEC level to:
- (a) ensure the performance of all offshore facility security tasks;
 - (b) control access to the offshore facility;
 - (c) monitor the offshore facility;
 - (d) monitor restricted areas to ensure that only authorized persons have access;
 - (e) supervise the handling of ships' stores and industrial supplies;
 - (f) ensure that security communication is readily available; and,
 - (g) ensure the security of interfacing with vessels.
- (2) An offshore facility security plan shall contain security procedures to ensure that a supply vessel that is en route between a marine facility and the offshore facility while the offshore facility is undergoing a MARSEC level change is informed of the change by the offshore facility security officer and takes appropriate action to harmonize its MARSEC level to correspond with that of the offshore facility before entering the offshore facility security zone.
- (3) An offshore facility security plan shall contain security procedures to ensure that, when notified of an increase in MARSEC level, the offshore facility security officer informs all offshore facility personnel about identified security threats, emphasizes reporting procedures and stresses the need for increased vigilance.
- (4) An offshore facility security plan shall contain security procedures to ensure that the operator of the offshore facility informs the Chief Safety Officer as soon as possible after becoming aware that the offshore facility is not in compliance with the requirements of this section.

Security Procedures for Access Control

29. (1) An offshore facility security plan shall contain security procedures for each MARSEC level to control access to the offshore facility including:
- (a) preventing access to restricted areas;
 - (b) establishing a restricted area at the offshore facility for conducting screening of persons and goods;
 - (c) establishing a means to ensure that personnel at the offshore facility are authorized to remain there if there is an increase in the MARSEC level; and,
 - (d) establishing a means to respond to the presence of unauthorized persons at the offshore facility.
- (2) The security procedures shall not require offshore facility personnel to screen other offshore facility personnel or their goods.
- (3) The security procedures shall be designed to ensure, for any place that serves as a point of embarkation for the offshore facility, that:
- (a) there is a place designated as a restricted area for the conduct of screening;
 - (b) there is fencing or other barriers for the restricted area;
 - (c) there are signs, in English and French and conspicuously posted, that describe the security procedures in effect and clearly state that
 - (i) boarding the offshore facility or entering the screening area, if coming from a landside facility with security procedures and equipment for access control approved in the offshore security plan, will provide consent for authorized screening, and,
 - (ii) the failure to consent to screening will result in the denial of access to the offshore facility;
 - (d) there are separate zones for persons and goods that have been screened;
 - (e) the unauthorized introduction of weapons, explosives and incendiaries is deterred;
 - (f) weapons, explosives and incendiaries that are authorized by the operator to be at the offshore facility are secured; and,
 - (g) there are identification systems that allow for temporary or permanent identification of offshore facility personnel and visitors.

- (4) The security procedures and equipment required for their implementation shall be specified in the offshore facility security plan in detail. The plan may set out that the procedures are to be effected at a shoreside point of embarkation or at the offshore facility, but in all cases shall, for each MARSEC level, shall specify the type of restriction or prohibition to be applied and the means of enforcing it.
 - (5) The security procedures may set out in full or may reference an approved marine facility security plan if the marine facility serves as the point of embarkation.
30. (1) An offshore facility security plan shall contain security procedures for restricted areas for each MARSEC level and shall:
- (a) identify the restricted areas;
 - (b) identify the persons who are authorized to have access to each restricted area;
 - (c) set out the conditions under which access may take place;
 - (d) define the extent of each restricted area; and,
 - (e) set out the times when access restrictions apply.
- (2) Areas containing any of the following shall be designated in the plan as restricted areas:
- (a) security-sensitive information;
 - (b) security and surveillance equipment and systems and their controls and lighting system controls;
 - (c) critical offshore facility infrastructure equipment such as
 - (i) water supplies,
 - (ii) telecommunications,
 - (iii) power distribution systems, and,
 - (iv) access points for ventilation and air conditioning systems;
 - (d) manufacturing areas and control rooms;
 - (e) areas designated for loading, unloading or storage of stores and industrial supplies;
 - (f) areas containing hazardous materials; and,
 - (g) areas containing dangerous goods, including certain dangerous cargoes.
31. (1) An offshore facility security plan shall contain security procedures for the delivery of ships' stores and industrial supplies for each MARSEC level that set out the restrictions or prohibitions applying at the point of embarkation or offshore facility and the means of applying them and may include procedures to:
- (a) check package integrity;
 - (b) refuse acceptance unless the packages have been ordered and screened; and,
 - (c) deter tampering.
- (2) Security procedures for the delivery of ships' stores and industrial supplies may be made by reference to a marine facility security plan for a marine facility if the marine facility serves as the point of embarkation.
- (3) For MARSEC LEVEL 1, the security procedures shall be designed to ensure that deliveries of ships' stores and industrial supplies:
- (a) match the order before being loaded; and,
 - (b) are stowed securely immediately.
- (4) For MARSEC level 2, the security procedures shall be additional to those at MARSEC level 1 and may include procedures to intensify the checking of ships' stores and industrial supplies during delivery.
- (5) For MARSEC level 3, the security procedures shall be additional to those at MARSEC level 1 and MARSEC level 2 and may include procedures for:
- (a) checking ships' stores and industrial supplies more extensively; and,
 - (b) restricting, suspending or refusing the delivery of ships' stores and industrial supplies.
32. (1) An offshore facility security plan shall contain security procedures for monitoring the offshore facility, including its security zones, restricted areas, and surrounding areas, shall specify the means to be used and may include a combination of:
- (a) lighting;
 - (b) watchkeepers;
 - (c) deck watches;
 - (d) Waterborne patrols; and,
 - (e) surveillance equipment.
- (2) For MARSEC level 2, the security procedures for monitoring shall be additional to those established at MARSEC level 1 and shall include:
- (a) conducting emergency searches of the offshore facility;

- (b) increasing the coverage and intensity of lighting and surveillance equipment, including the provision of additional lighting and surveillance;
 - (c) increasing the number of watchkeepers and monitoring personnel; and,
 - (d) if waterborne patrols are provided, coordinating with them.
- (3) For MARSEC level 3, the security procedures for monitoring shall be additional to those established at MARSEC level 1 and MARSEC level 2 and shall include:
- (a) switching on all lighting, or illuminating the vicinity, of the offshore facility;
 - (b) switching on of all on-board surveillance equipment capable of recording activities on or in the vicinity of the offshore facility;
 - (c) maximizing the length of time that surveillance equipment can continue to record; and,
 - (d) preparing for underwater inspection of the offshore facility.
33. (1) An audit of an offshore facility security plan shall take into account the most recent offshore facility security assessment and determine whether there are any deficiencies or changes — such as in security threats, procedures, or responsibilities or in personnel, operations or operator — that require amendments to be made to the plan.
- (2) An audit is conducted:
- (a) annually — and no later than one year after the date of approval of the plan — over the entire plan; and,
 - (b) whenever there is a new operator of the offshore facility, a change in operations or location or modifications to the offshore facility that would affect its security.
- (3) Persons conducting an audit shall have knowledge of the methods of conducting audits, and inspections and of control and monitoring techniques and, if possible, be independent of the activities being audited.
- (4) If the results of an audit require an amendment to the offshore facility security assessment or plan, the offshore facility security officer shall prepare an amendment for approval
- (5) The company security officer shall submit to the Chief Safety Officer for approval within 30 days after completion of the audit any amendment to the offshore facility security plan that is required.
- (6) The operator of the offshore facility may submit to the Chief Safety Officer other proposed amendments to the offshore facility security plan. The proposed amendments shall be submitted at least 30 days before they are to take effect.
- (7) The operator of the offshore facility shall, within 60 days after the Chief Safety Officer informs the operator in writing that the offshore facility security plan no longer meets the requirements to remain approved, ensure that proposed amendments are submitted for approval.
- (8) If proposed amendments are submitted under subsection (4) or (7) and the amended plan is not approved, the plan ceases to be valid on the day on which the operator of the offshore facility receives notification that the plan is not approved.
- (9) The offshore facility security officer shall attach to the plan a letter from the Chief Safety Officer that certifies that the plan meets these requirements.
34. The company security officer of an offshore facility shall submit an offshore facility security plan to the Chief Safety Officer for approval.
35. (1) The Chief Safety Officer shall approve an offshore facility security plan that meets the requirements, unless approving the plan is not in the public interest and is likely to adversely affect marine security.
- (2) Subject to subsection 33(8), the Chief Safety Officer shall determine the period of validity of the plan after taking into account [Note: the criteria for the Chief Safety Officer’s fixing of the period are to be determined. These criteria may, for example, be the record of the operator of the offshore facility with respect to their conformity with statutory or regulatory requirements, where the record may have an impact on the security of marine transportation, as well as the complexity of the security plan to be approved, in terms of the number of procedures and extent of detail it contains, etc.]