CAYMAN ISLANDS SHIPPING REGISTRY

3rd Floor, Kirk House,
22 Albert Panton Street
P.O. Box 2256, George Town
Grand Cayman,
Cayman Islands.

Fax: (1 345) 949 8849
Tel: (1 345) 949 8831
E-mail: cisr@candw.ky
Web site: www.caymarad.org

Shipping Notice CISN 08/05

Minimum Requirements for Ship Security Assessments (SSA) and Ship Security Plans (SSP)

To: OWNERS, MANAGERS, COMPANY SECURITY OFFICERS, MASTERS AND SHIP SECURITY OFFICERS of CAYMAN ISLANDS SHIPS

---

1. Background

1.1. Compliance with Chapter XI-2 of SOLAS and the ISPS Code has been mandatory on qualifying ships[1] since 1 July 2004.

1.2. The introduction of the ISPS Code represented a huge challenge for all involved, and one which was generally met with both commitment and professionalism.

1.3. Ship Security Plans (SSP) specifically developed to meet the requirements of the ISPS Code started to be implemented onboard ships during 2003 and now all qualifying ships are implementing an approved SSP.

1.4. During this period experience with implementing the ISPS Code has continued to grow. IMO has published guidance on implementation and has agreed many interpretations of the requirements of the Code itself.

1.5. Based on the knowledge gained during implementation (which includes evaluating the effectiveness of approved SSPs during onboard verifications), the Cayman Islands Shipping Registry has now published "Minimum Requirements for Ship Security Assessments and Ship Security Plans".

1.6. These "Minimum Requirements" do not constitute any additional requirements beyond those contained in the ISPS Code, rather they clarify what is expected to meet the Code requirements.

2. Timetable

2.1. The "Minimum Requirements" will be applied to all Ship Security Plans which are submitted for initial approval after 01 July 2005.

---

[1] In the context of this Shipping Notice the term "ship" is used to refer to any vessel which is subject to SOLAS XI-2 and the ISPS Code.

3. **Ship Security Assessment**

3.1. See Appendix 1 & 3 of this Shipping Notice.

4. **Ship Security Plan**

4.1. See Appendix 2 of this Shipping Notice.

5. **Previously approved Ship Security Plans**

5.1. The majority of currently approved SSPs will not require any amendments to meet the "Minimum Requirements".

5.2. Ship Security Plans which have been approved prior to 1 July 2005 **do not** need to be re-submitted for approval against these "Minimum Requirements".

5.3. When submitting routine amendments to an approved SSP for approval, Company Security Officers must review these amendments against the "Minimum Requirements".

5.4. When SSPs are periodically reviewed by the company in accordance with ISPS A/9.4.11, the "Minimum Requirements" should be taken into account when deciding if updating of the SSP is warranted.

5.5. Existing SSPs will be evaluated against these "Minimum Requirements" during the onboard verifications required by Section A/19 of the ISPS Code. If the SSP is not found to comply with the "Minimum Requirements" this will be brought to the attention of the CSO.

Minimum Requirements for Ship Security Assessments

1. **Application of ISPS Code Part B**

   a. In general personal involved in conducting Ship Security Assessments are encouraged to use the methodology and guidance set out in the United States Coast Guard (Navigation and Vessel Inspection Circular NVIC 10-2) which for the sake of completeness has been included in Appendix 3 of this Shipping Notice

   b. ISPS Code Part B Paragraphs 8.1 to 13.8 must be fully taken into account when conducting Ship Security Assessments (SSA) and developing Ship Security Plans (SSP). Not all paragraphs will be applicable to every ship. Where a paragraph is not considered applicable or suitable, the company submitting the SSA and SSP should be able to justify the paragraph's exclusion.

   c. Example: Paragraph B/9.40 calls for 100% x-ray screening of unaccompanied baggage at Security Level 3. This will be impractical for many ships to implement and so it would be acceptable not to implement these measures provided the ship does not to accept unaccompanied baggage onboard at this Security Level or if screening equivalent to the guidance given in B/9.40 is employed.

2. **Conducting Ship Security Assessments**

   a. Ship Security Assessments should be conducted by persons with appropriate skills to evaluate the security of a ship. As a general rule, those conducting SSAs should have completed a recognised Company Security Officers training course. Other qualifications and experience will be accepted on a case by case basis.

   b. Evidence of qualification of those conducting SSAs should be included with the SSA when it is submitted with the SSP.

   c. It is acceptable to follow standard methodologies[2] for conducting SSAs provided that all requirements for the SSA are addressed (See also "Application of ISPS Code Part B", above).

3. **Fleet Wide Ship Security Assessments**

   a. It is recognised that there will be similarities between both the threats present and the mitigation measures applied between ships operated by a single company. It is acceptable to conduct a "fleet wide" SSA, provided the individual characteristics of each ship is addressed (probably during the on-scene security survey and individual SSA Report).

4. **Threat Assessments**

   a. Threat assessments form an important part of conducting SSAs. Generally threats are categorised as a function of their likelihood to occur and the consequences should they occur. Although this is a mainly qualitative process, the SSA should contain sufficient justification to validate each decision reached.

   b. The threat assessment should be *a "systematic and analytical process to consider the likelihood that a security breach will endanger an asset, individual or function"* and

[2] Examples include those available from Classification Societies, Industry Groups, Administrations, etc

should *"identify actions to reduce the vulnerability and mitigate the consequences of a security breach"*. Threat assessments which consist solely of unsupported "tick boxes" will not be accepted.

5. **On-scene Security Survey**

   a. The on-scene security survey is an essential element of conducting any SSA. By definition, the on-scene security survey must be conducted onboard each ship.

   b. It is unlikely that any ship will have a valid reason for excluding the guidance given in ISPS B/8.6 (identified points of access to and within the ship) or ISPS B/8.14.1 - 7 (on-scene security survey) from the SSA.

6. **Ship Security Assessment Report.**

   a. The SSA must accompany the SSP for approval in the form of a written report which is to include:

      i. A summary of how, when and by who the SSA was conducted.

      ii. The findings of the on-scene security survey.

      iii. A description of each vulnerability identified.

      iv. Proposed countermeasures to be included in the SSP.

   b. The report should contain evidence that the assessment has been reviewed and accepted by the company.

Minimum Requirements for Ship Security Plans

1. **Application of ISPS Code Part B**
   a. ISPS Code Part B Paragraphs 8.1 to 13.8 must be fully taken into account when conducting Ship Security Assessments (SSA) and developing Ship Security Plans (SSP). Not all paragraphs will be applicable to every ship. Where a paragraph is not considered applicable or suitable, the company submitting the SSA and SSP should be able to justify the paragraph's exclusion.
   b. Example: ISPS B/13.6 calls for the Drills & Exercises required by ISPS A/9.4.9 to include those threats identified in ISPS B/8.9. Not all of these threats will be appropriate to every ship. Should any of these threats not be included in the program of Drills and Exercises, the justification for their exclusion should be included in either the SSA or SSP.
2. **Requirements for Procedures**
   a. The ISPS Code requires several procedures to be included in the SSP (ISPS A/9.4). When a procedure is required, a procedure must be included.
   b. A procedure is not a simple re-statement of a Code requirement. A procedure must contain sufficient detail to make it clear as to how the requirement will be met.
   c. Example: ISPS A/9.4.8 requires *"procedures for the auditing of security activities"*. A statement in the SSP that *"Internal Audits will be conducted annually"* does not constitute a procedure and will not be accepted as meeting the requirements of ISPS A/9.4.8.
   d. As a general guide: Procedures should make the following clear:
      i. What is to be achieved?
      ii. Who does it?
      iii. How is it done?
      iv. When is it done?
      v. What controls are in place to ensure it is done properly?
      vi. What records of the activity are kept?
3. **The SSP should be a Stand Alone Document**
   a. It is not permissible to reference other documentation (that does not form part of the SSP) as meeting a requirement for the SSP.
   b. Example: If the SSP states that *"Evacuation in case of security threats or breaches of security will be conducted in accordance with Proc XXX of the Safety Management System"* then the relevant procedure from the Safety Management System must be included as part of the SSP that is submitted for approval.
4. **Master's Overriding Authority**
   a. The SSP must contain a statement confirming the master's overriding authority for safety and security onboard. This statement must also confirm that masters may seek assistance from the Company or any Contracting Government as they feel appropriate.

It is acceptable to use the same wording as contained in ISPS A/6.1 to meet this requirement in the SSP.

5. **Access Control**

   a. SSPs should recognise that **properly identified** "Duly Authorised Officers of Contracting Governments" and their belongings are not subject to search prior to boarding and can not be denied access to the ship. This is clearly stated in SOLAS XI-2/8.1.

   b. Further details are contained in Cayman Islands Security Advisory 02/04.

6. **Identification of the Ship Security Officer (SSO)**

   a. The SSP must identify the SSO by either name or position (rank) onboard. It is not permissible to only state that the SSO will be a suitably qualified member of the ship's crew.

   b. The SSO should have sufficient authority onboard to enable the duties and responsibilities of the SSO to be effectively discharged.

   c. It is permissible for the master to also act as the SSO.

7. **Declarations of Security**

   a. The SSP should state that the ship is to request a Declaration of Security in all circumstances specified in ISPS A/5.2.

8. Records

   a. The SSP must specify how requirements for records contained in ISPS A/10 will be met.

   b. The SSP should state that all records required by SOLAS XI-2 or the ISPS Code are to be retained onboard for a period of not less than 3 years.

   c. The SSP must ensure that the records required by SOLAS XI-2/2.3 covering at least the last 10 calls at port facilities are available for inspection by Port State Control Officers.

9. Ship Security Alert System

   a. Procedures included in the SSP to meet the requirements of ISPS A/9.4.17 -18 must be compatible with the provisions of Cayman Islands Shipping Notice 01/05 (Ship Security Alert Systems), or its replacement.

   b. If the competent authority for receiving security alerts (See SOLAS XI-2/6.2.1) is not the Company, details of this competent authority and communication protocols must be included in the SSP.

Appendix 3:
Extract From The United States Coast Guard Navigation and Vessel Inspection Circular NVIC 10-2

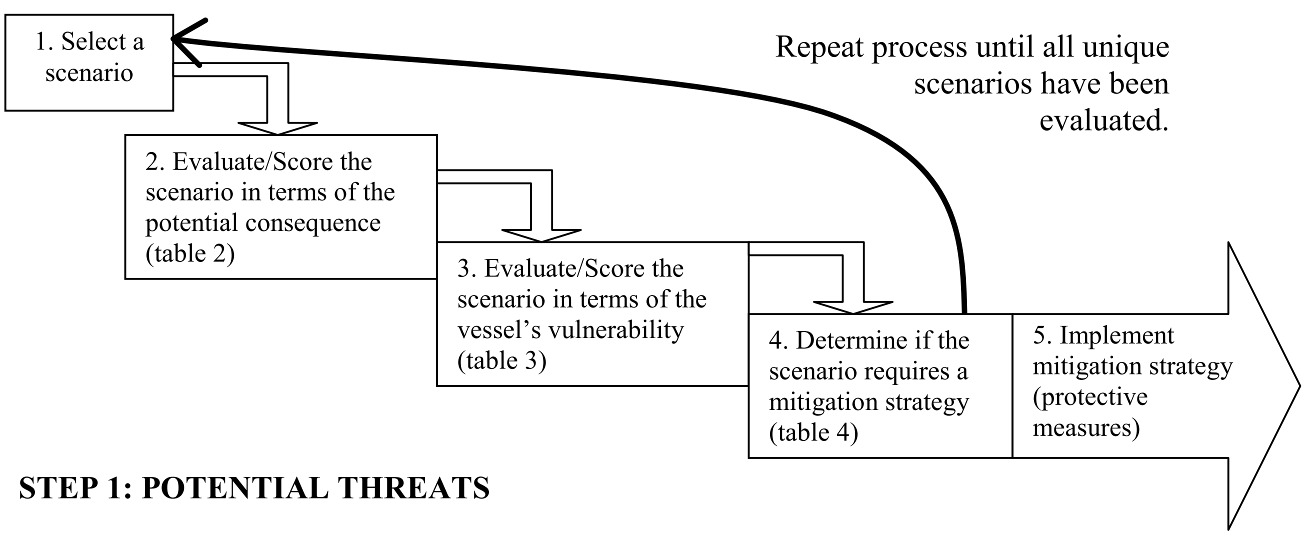
Appendix B

Guidance on Performing Security Assessments

It is generally agreed that risk-based decision-making is one of the best tools to complete a security assessment and to determine appropriate security measures for a vessel. Risk-based decision-making is a systematic and analytical process to consider the likelihood that a security breach will endanger an asset, individual, or function and to identify actions to reduce the vulnerability and mitigate the consequences of a security breach.

A security assessment is a process that identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may lead to a security breach, and may suggest options to eliminate or mitigate those weaknesses. For example, a security assessment might reveal weaknesses in an organization's security systems or unprotected access points such as the pilot boarding ladder not being raised or side ports not being secured or monitored after loading stores. To mitigate this threat, a vessel would implement procedures to ensure that such access points are secured and verified by some means. Another security enhancement might be to place locking mechanisms and/or wire mesh on doors and windows that provide access to *restricted areas* to prevent unauthorized personnel from entering such spaces. Such assessments can identify vulnerabilities in vessel operations, personnel security, and physical and technical security.

The following is a simplified risk-based security assessment that can be further refined and tailored to specific vessels. The process and results may be documented when performing the assessment. An example is provided in Table 5 on how to document the process and results.



STEP 1: POTENTIAL THREATS

To begin an assessment, a vessel or company needs to consider attack scenario(s) consisting of a potential threat to the vessel under specific circumstances. It is important that the scenario or scenarios are within the realm of possibility and, at a minimum, address known capabilities and intents as given by a threat assessment. For example, a boat containing explosives (a specific attack scenario) ramming a tanker (target) that is outbound through a choke point (specific circumstance) is one credible scenario. It may be less credible that a hand held missile launched from a distance at a large tanker could intentionally sink the vessel that is outbound through a choke point.

The number of scenarios is left to the judgment of the vessel owner and/or *operator*. An initial evaluation should at least consider those scenarios provided in Table 1 with emphasis being placed on the worst-case scenario, and the most probable scenarios. Care should be taken to avoid unnecessarily evaluating excessive scenarios that result in low consequences. Minor variations of the same scenario also do not need to be evaluated separately unless there are measurable differences in consequences.

Table 1: Notional List of Scenarios

Typical Types of Scenarios		Application Example
1. Intrude and/or take control of the target and ...	a. Damage/destroy the vessel with explosives	Intruder plants explosives.
	b. Damage/destroy the vessel through malicious operations/acts	• Intruder takes control of a vessel and runs it aground or collides with something intentionally. • Intruder intentionally opens valves to release Hazmat, etc.
	c. Create a hazardous or pollution incident without destroying the vessel	• Intruder opens valves/vents to release toxic materials or releases toxic material brought along. • Intruder overrides interlocks leading to damage/destruction.
	d. Take hostages/kill people	Goal of the intruder is to kill people.
2. Externally attack the vessel by …	a. Moving explosives adjacent to vessel • From the waterside • On the shore side • Subsurface	• USS Cole style attack. • Car/truck bomb.
	b. Ramming a stationary target: • With a vessel • With a land-based vehicle	Intentional allision meant to damage/destroy the target (i.e. waterway choke point). NOTE: Evaluate overall consequences from the allision, but only evaluate the vulnerabilities of the vessel and not the vulnerabilities of the target being rammed.
	c. Launching or shooting weapons from a distance	Shooting at a vessel using a rifle, missile, etc.
3. Use the vessel as a means of transferring …	a. Materials to be used as a weapon into/out of the country	
	b. People into/out of the country	

STEP 2: CONSEQUENCE ASSESSMENT

Each scenario should be evaluated in terms of the potential consequences of the attack. Three elements are included in the consequence assessment: death and injury, economic impact, and environmental impact. A descriptor of the consequence components follows:

DEATH AND INJURY	The potential number of lives that could be lost and injuries occurring as a result of an attack scenario.
ECONOMIC IMPACT	The potential economic impact of an attack scenario.
ENVIRONMENTAL IMPACT	The potential environmental impact of an attack scenario.

The appropriate consequence score or "rating", should be evaluated for each scenario. Consequence ratings and criteria with benchmarks are provided in the following table. These ratings are intended to be broad relative estimates. The appropriate rating is determined by using the consequence component that results in the highest rating. For example, if the death and injury and economic impact result in a Moderate or "1" rating but the environmental impact result is a Significant or "2" rating, then the over all consequence score would be assigned a rating of "2." A precise calculation of these elements is not necessary.

Table 2: Consequence Score

Assign a rating of:	If the impact could be
3	CATASTROPHIC = numerous loss of life or injuries, major national or long term economic impact, complete destruction of multiple aspects of the eco-system over a large area
2	SIGNIFICANT = multiple loss of life or injuries, major regional economic impact, long-term damage to a portion of the eco-system
1	MODERATE = little or no loss of life or injuries, minimal economic impact, or some environmental damage

STEP 3: VULNERABILITY ASSESSMENT

Each scenario should be evaluated in terms of the vessel's vulnerability to an attack. Four elements of the vulnerability score are: availability, accessibility, organic security, and vessel hardness. With the understanding that the vessel owner and/or *operator* has the greatest control over the accessibility and organic security elements, these elements may be addressed for each scenario. Descriptors of these two vulnerability elements follow:

ACCESSIBILITY	Accessibility of the vessel to the attack scenario. This relates to physical and geographic barriers that deter the threat without organic security.
ORGANIC SECURITY	The ability of security personnel to deter the attack. It includes security plans, communication capabilities, guard force, intrusion detection systems, and timeliness of outside law enforcement to prevent the attack.

The vessel owner and/or *operator* should discuss each vulnerability element for a given scenario. The initial evaluation of vulnerability is normally viewed with only existing strategies and protective measures, meant to lessen vulnerabilities, which are already in place. After the initial evaluation has been performed, a comparison evaluation can be made with new strategies and protective measures considered. Assessing the vulnerability with only the existing strategies and protective measures provides a better understanding of the overall risk associated with the scenario and how new strategies and protective measures will mitigate risk.

The vulnerability score and criteria with benchmark examples are provided in the following table. Each scenario should be evaluated to get the individual score for each element and then sum these elements to get the total vulnerability score (step 3 in Table 5). This score should be used as the vulnerability score when evaluating each scenario in the next step.

Table 3: Vulnerability Score

Category	Accessibility	Organic Security
3	No deterrence (e.g. unrestricted access to vessel and unrestricted internal movement)	No deterrence capability (e.g. no plan, no guard force, no emergency communication, outside law enforcement not available for timely prevention, no detection capability)
2	Good deterrence (e.g. single substantial barrier; unrestricted access to within 100 yards of vessel)	Good deterrence capability (e.g. minimal security plan, some communications, armed guard force of limited size relative to the vessel; outside law enforcement not available for timely prevention, limited detection systems)
1	Excellent deterrence (expected to deter attack; access restricted to within 500 yards of vessel; multiple physical/geographical barriers)	Excellent deterrence capability expected to deter attack; covert security elements that represent additional elements not visible or apparent)

STEP 4: MITIGATION

The vessel owner and/or *operator* should next determine which scenarios may have mitigation strategies (protective measures) implemented. This is accomplished by determining where the scenario falls in Table 4 based on the consequence and vulnerability assessment scores. Following are terms used in Table 4 as mitigation categories:

“Mitigate” means that mitigation strategies, such as security protective measures and/or procedures, may be developed to reduce risk for that scenario. An appendix to the *Vessel Security Plan* may contain the scenario(s) evaluated, the results of the evaluation, a description of the mitigation measure evaluated, and the reason mitigation measures were or were not chosen.

"Consider" means that the scenario should be considered and mitigation strategies should be developed on a case-by-case basis. The *Vessel Security Plan* may contain the scenario(s) evaluated, the results of the evaluation, and the reason mitigation measures were or were not chosen.

"Document" means that the scenario may not need a mitigation measure at this time and therefore needs only to be documented. However, mitigation measures having little cost may still merit consideration. The security plan may contain the scenario evaluated and the results. This will be beneficial in further revisions of the security plan, to know if the underlying assumptions have changed since the last edition of the security assessment.

Table 4 is intended as broad, relative tool to assist in the development of the vessel security plan. "Results" are not intended to be the sole basis to trigger or waive the need for specific measures, but are one tool in identifying potential vulnerabilities and evaluating prospective methods to address them.

Table 4: Vulnerability & Consequence Matrix

		Total Vulnerability Score		
		2	3-4	5-6
Consequence Score	3	Consider	Mitigate	Mitigate
	2	Document	Consider	Mitigate
	1	Document	Document	Consider

To assist the vessel owner and/or *operator* in determining which scenarios may require mitigation methods, the vessel owner and/or *operator* may find it beneficial to use Table 5 provided below. The vessels owner and/or *operator* can record the scenarios considered, the consequence score (Table 2), outcome of the each element of vulnerability (Table 3), the total vulnerability score, and the mitigation category Table 4).

Table 5

MITIGATION DETERMINATION WORKSHEET					
Step 1	Step 2	Step 3			Step 4
Scenario/Description	Consequence Score (Table 2)	Vulnerability Score (Table 3) Accessibility	+ Organic Security	= Total Score	Mitigation Results (Table 4)

STEP 5: IMPLEMENTATION METHODS

The true value of these assessments is realized, once the vessel owner and/or *operator* determines which scenarios require mitigation, when mitigation strategies (protective measures) are implemented to reduce vulnerabilities. The overall desire is to reduce the risk associated with the identified scenario. Note that generally, as mentioned previously, it is easier to reduce vulnerabilities than to reduce consequences or threats when considering mitigation strategies.

To assist the vessel owner and/or *operator* in evaluating the effectiveness of specific mitigation strategies (protective measures), the vessel owner and/or *operator* may find it beneficial to use Table 6 provided below.

Table 6

MITIGATION IMPLEMENTATION WORKSHEET						
1	2	3	4			5
Mitigation Strategy (Protective Measure)	**Scenario(s) that are affected by Mitigation Strategy (from Step 1 in Table 5)**	**Consequence Score (remains the same)**	**New Vulnerability Score (Table 3)**			**New Mitigation Results (Table 4)**
			Accessibility +	**Organic Security =**	**Total Score**	
1.	1.					
	2.					
	…					
2.	…					

The following steps correspond to each column in Table 6.

1. The vessel owner and/or *operator* should brainstorm mitigation strategies (protective measures) and record them in the first column of Table 6.

2. Using the scenario(s) from Table 5, list all of the scenario(s) that would be affected by the selected mitigation strategy.

3. The consequence score remains the same as was recorded in Table 5 for each scenario.

4. Re-evaluate the vulnerability score (Table 3) for each element, taking into consideration the mitigation strategy, for each scenario.

5. With the consequence score and new total vulnerability score, use Table 4 to determine the new mitigation results.

There are two factors, effectiveness and feasibility, to consider in determining if a mitigation strategy should be implemented. A strategy may be thought of as highly effective if its implementation lowers the mitigation category (e.g. from “mitigate” to "consider" in Table 4). A strategy may be thought of as partially effective if the strategy will lower the overall vulnerability score when implemented by itself or with one or more other strategies. For example, if a mitigation strategy lowers the vulnerability score from "5-6" to "3-4" while the consequence score remains at "3" and the mitigation category stays at "mitigate."

It should be noted that if a mitigation strategy, when considered individually, does not reduce the vulnerability, that multiple strategies may be considered in combination. Considering mitigation strategies as a whole may allow the vulnerability to be reduced.

A strategy may be thought of as feasible if it can be implemented with little operational impact or funding relative to the prospective reduction in vulnerability. A strategy may be thought of as partially feasible if its implementation requires significant changes or funding relative to the prospective reduction in vulnerability. A strategy may be thought of as not feasible if its implementation is extremely problematic or is cost prohibitive.

The vessel owner and/or *operator* should keep in mind that some strategies may be deployed commensurate with various security threat levels established. Feasibility of a mitigation strategy may vary based on the *MARSEC level*, therefore some strategies may not be warranted at *MARSEC Level 1*, but may be at *MARSEC Levels 2* or 3. For example, using divers to inspect the underwater pier structures and vessel may not be necessary at *MARSEC Level I*, but may be necessary if there is a specific threat and/or an increase in *MARSEC level*. Mitigation strategies should ultimately ensure that a level of security is maintained to achieve the objectives discussed in enclosure (1).

As an example of a possible vulnerability mitigation measure, a company may implement security patrols by hiring additional personnel to detect and prevent unauthorized persons from entering spaces below the main deck on a passenger ferry. This measure would improve organic security and may reduce the overall vulnerability score from a "high" to a "medium". This option, however, is specific for this scenario and also carries a certain cost. Another option might be to secure all access points to spaces below the main deck. This may reduce the accessibility score from "high" to "medium". This option does not require additional personnel and is a passive mitigation measure. Similarly, other scenarios can be tested to determine the most effective strategies.

The vessel owner and/or *operator* should develop a process through which overall security is continually evaluated by considering consequences and vulnerabilities, how they may change over time, and what additional mitigation strategies can be applied.