

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

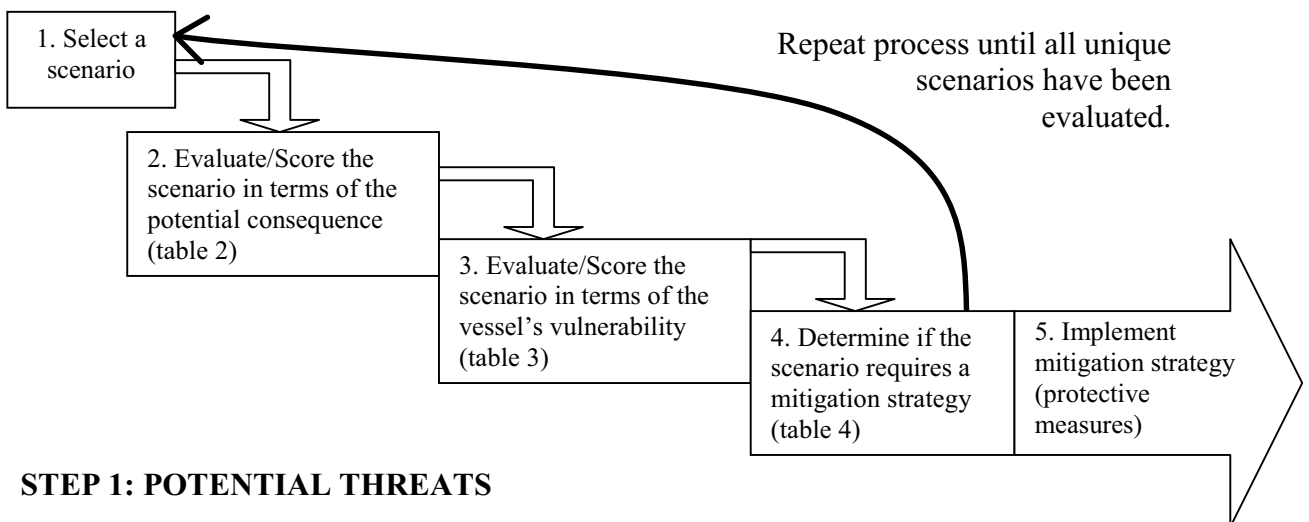
## Appendix B

### 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
<b>1. Intrude and/or take control of the target and ...</b>	a. Damage/destroy the vessel with explosives	Intruder plants explosives.
	b. Damage/destroy the vessel through malicious operations/acts	<ul style="list-style-type: none"> <li>• Intruder takes control of a vessel and runs it aground or collides with something intentionally.</li> <li>• Intruder intentionally opens valves to release Hazmat, etc.</li> </ul>
	c. Create a hazardous or pollution incident without destroying the vessel	<ul style="list-style-type: none"> <li>• Intruder opens valves/vents to release toxic materials or releases toxic material brought along.</li> <li>• Intruder overrides interlocks leading to damage/destruction.</li> </ul>
	d. Take hostages/kill people	Goal of the intruder is to kill people.
<b>2. Externally attack the vessel by ...</b>	a. Moving explosives adjacent to vessel <ul style="list-style-type: none"> <li>• From the waterside</li> <li>• On the shore side</li> <li>• Subsurface</li> </ul>	<ul style="list-style-type: none"> <li>• USS Cole style attack.</li> <li>• Car/truck bomb.</li> </ul>
	b. Ramming a stationary target: <ul style="list-style-type: none"> <li>• With a vessel</li> <li>• With a land-based vehicle</li> </ul>	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.
<b>3. Use the vessel as a means of transferring ...</b>	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:

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

<b>Assign a rating of:</b>	<b>If the impact could be</b>
<b>3</b>	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
<b>2</b>	SIGNIFICANT = multiple loss of life or injuries, major regional economic impact, long-term damage to a portion of the eco-system
<b>1</b>	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:

<b>ACCESSIBILITY</b>	Accessibility of the vessel to the attack scenario. This relates to physical and geographic barriers that deter the threat without organic security.
<b>ORGANIC SECURITY</b>	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)			Mitigation Results (Table 4)
		Accessibility	Organic Security	Total Score	

### 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	Total Security 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 1*, 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.