U.S. Department of Homeland Security
United States Coast Guard

Commandant
U.S. Coast Guard

2100 2nd Street SW
Washington, DC 20593-0001
Staff Symbol: G-MP
Phone: 202-366-9991
FAX: 202-366-9999

COMDTPUB P16700.4
NVIC 11-02 Change 1

AUG 6 2004

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 11-02, CHANGE 1

Subj: CH-1 TO NVIC 11-02, RECOMMENDED SECURITY GUIDELINES FOR FACILITIES

1. PURPOSE.

This document revises Navigation and Vessel Inspection Circular (NVIC) No. 11-02 by purging outdated sections and inserting changes. With these changes in place, this Circular only provides the guidance for performing Facility Security Assessments.

2. BACKGROUND

As the leader in Maritime Homeland Security, the Coast Guard has taken many measures to detect, deter, disrupt, and respond to attacks against U.S. territory, population, vessels, facilities, and critical maritime infrastructure. NVIC 11-02 was published to provide port users the necessary guidance to conduct vulnerability assessments and to develop security plans. In the two years following the terrorist events of September 11, 2001, the Maritime Transportation Security Act of 2002 (MTSA) was enacted into law and associated regulations were published on October 22, 2003. The backbone of the regulations superceded the guidance provided in the various elements of the original NVIC and a large portion of the NVIC will be removed. The portion of the NVIC being retained is the section, referenced in the regulations, that provides guidance for conducting facility security assessments.

DISTRIBUTION – SDL No. 140

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B		2	10		1			1						132	1			1								30
C												1														
D	1	1		1							1															
E															1											
F																										
G																										
H																										

*NON-STANDARD DISTRIBUTION: B:a Commandant (G-MP/G-MOC/MO-1//MSE/MW/OPD/OPL/OPF-3) (1)

3. DISCUSSION.

Under Title 33, Parts 104.305, 105.305, and 106.305 of the Code of Federal Regulations, the requirement for conducting assessments is a responsibility of vessel and facility owners. The Coast Guard is issuing, through means of this NVIC, recommended criteria for performing the required assessments. Enclosure (1) outlines procedures to evaluate and document security measures. It is a simplified risk-based security assessment tool, which can be used to refine and tailor security measures to specific facilities or to assess the equivalency of alternative approaches. Owners or operators are encouraged to document the process, record the results of these assessments and provide suggestions on how this assessment tool might be improved.

4. IMPLEMENTATION.

Make the following changes to the subject NVIC:

a. Remove pages 1- 7 of NVIC 11-02 and insert pages 1 and 2 of NVIC 11-02 CH 1.
b. Remove Enclosures 1, 2, 3, and 4.
c. Designate Enclosure 5 as Enclosure 1.

T. H. GILMOUR
Rear Admiral, U.S. Coast Guard
Assistant Commandant for Marine Safety, Security
and Environmental Protection

Encl (1) Guidance on Assessing Facility Security Measures

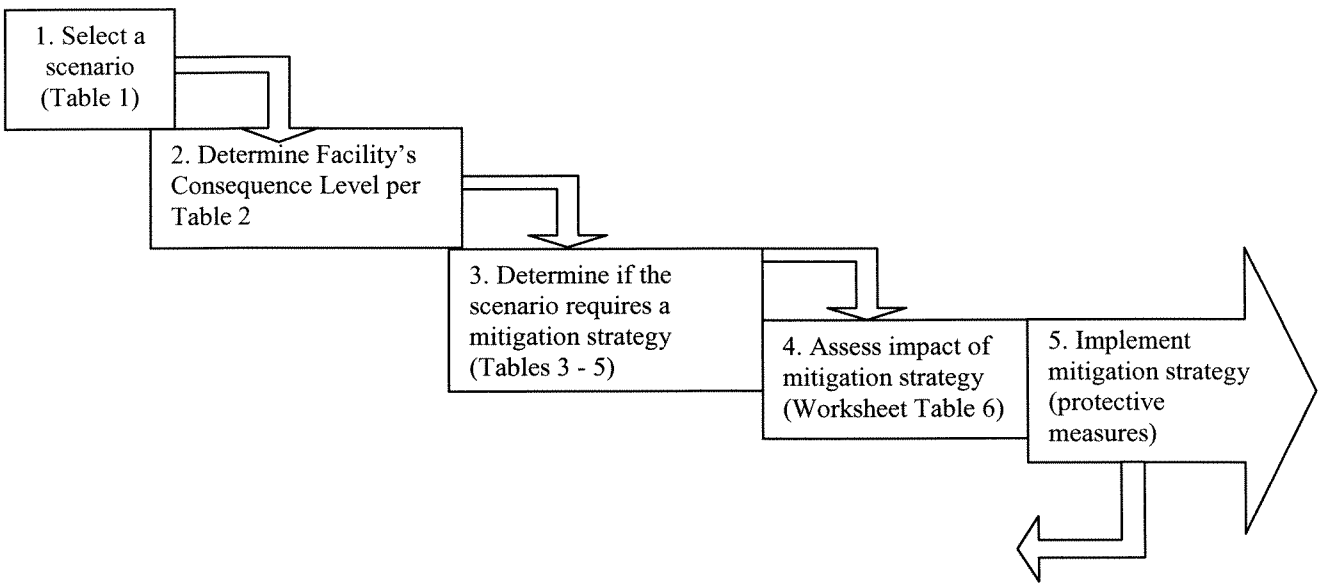
Guidance on Assessing Facility Security Measures

A security assessment performed in accordance with this enclosure may be used to evaluate the need for specific measures or evaluate alternate measures.

Risk-based decision-making is one of the best tools to perform a security assessment and to determine appropriate security measures for a facility. 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 that will reduce the vulnerability to 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 facility's perimeter not being lighted or gates not being secured or monitored after hours. To mitigate this vulnerability, a facility 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 facility operations, personnel security, and physical and technical security.

The following is a simplified risk-based security assessment, outlined in the following flow chart, which can be further refined and tailored to specific facilities. The process and results should be documented, (example provided in Table 5), when performing the assessment.



Note: Repeat process until all unique scenarios have been evaluated.

STEP 1: POTENTIAL THREATS

To begin an assessment, a facility or company needs to consider attack scenario(s) that consist of a potential threat to the facility 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. They should also be consistent with scenarios used to develop the Port Security Plan. For example, a bomb threat at a major petrochemical facility is one credible scenario. Table 1 provides a notional list of scenarios that may be combined with specific critical targets to develop the scenarios to be evaluated in the Facility Security Assessment.

The number of scenarios is left to the judgment of the facility or company. An initial evaluation should at least consider those scenarios provided in Table 1. Care should be taken to avoid unnecessarily evaluating an excessive number of 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
Intrude and/or take control of the target and ...	Damage/destroy the target with explosives	Intruder plants explosives.
	Damage/destroy the target through malicious operations/acts	Intruder takes control of a facility intentionally opens valves to release oil or hazmat that may then be ignited.
	Create a hazardous or pollution incident without destroying the target	Intruder opens valves/vents to release oil or toxic materials or releases toxic material brought along.
	Take hostages/kills people	Goal of the intruder is to kill people.
Externally attack the facility by ...	Launching or shooting weapons from a distance	Shooting at a target using a rifle, missile, etc to damage or destroy bulk storage tanks, dangerous cargo, etc.
Use the facility as a means of transferring ...	Materials, contraband, and/or cash into/out of the country	Facility is used as a conduit for Transportation security incidents
	People into/out of the country	

STEP 2: CONSEQUENCE ASSESSMENT

For this step a Facility Security Officer or company official should determine the appropriate consequence level (3, 2, or 1) determined from Table 2. The appropriate consequence level should be based on the "Description" of the facility (i.e., one that transfers, stores, or otherwise contains certain dangerous cargoes would have a "3" consequence level).

Table 2: Consequence Level

Consequence Level	Description
3	**Facilities that transfer, store, or otherwise handle a certain dangerous cargoes**
2	**Facilities that** **(1) Are subject to 33 CFR Parts 126 and 154 (other than certain dangerous cargoes);** **(2) Receive vessel(s) that are certificated to carry more than 150 passengers (other than those required to comply with 33 CFR 128); <u>or</u>** **(3) Receive vessels on international voyages including vessels solely navigating the Great Lakes**
1	**Facilities, other than those above.**

STEP 3: VULNERABILITY ASSESSMENT

Each scenario should be evaluated in terms of the facility's vulnerability to an attack. Four elements of vulnerability could be considered in the vulnerability score: availability, accessibility, organic security, and facility hardness, described as follows:

AVAILABILITY	The facility's presence and predictability as it relates to the ability to plan an attack.
ACCESSIBILITY	Accessibility of the facility 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.
FACILITY HARDNESS	The ability of the facility to withstand the specific attack based on the complexity of facility design and material construction characteristics.

The Facility Security Officer or company official should discuss each vulnerability element for a given scenario. The initial evaluation of vulnerability should be viewed with only existing strategies and protective measures, designed 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 will provide a better understanding of the overall risk associated with the scenario and how new strategies and protective measures will mitigate the risk.

With the understanding that the facility has the greatest control over the accessibility and organic security elements, this tool only takes into consideration these elements (not addressing availability or facility hardness) in assessing each scenario. The vulnerability score and criteria with benchmark examples are provided in the following table. Each scenario should be evaluated to get an accessibility and organic security score. 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

Score	Accessibility	Organic Security
3	No deterrence (e.g. unrestricted access to facility 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	Fair deterrence (e.g. single substantial barrier; unrestricted access to within 100 yards of bulk storage tanks)	Fair deterrence capability (e.g. minimal security plan, some communications, security force of limited size relative to the facility; outside law enforcement with limited availability for timely prevention, limited detection systems)
1	Good deterrence (expected to deter attack; access restricted to within 500 yards of bulk storage tanks; multiple physical/geographical barriers)	Good deterrence capability expected to deter attack (e.g., detailed security plan, effective emergency communications, well trained and equipped security personnel; multiple detection systems [camera, x-ray, etc.], timely outside law enforcement for prevention).

STEP 4: MITIGATION

The facility or company should next determine which scenarios should have mitigation strategies (protective measures) implemented. This is accomplished by determining where the scenario falls in Table 4 based on the consequence level and vulnerability assessment score. Table 4 is intended as a broad, relative tool to assist in the development of the Facility 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.

The following terms are used in Table 4 as mitigation categories:

"Mitigate" means that mitigation strategies, such as security protective measures and/or procedures, should be developed to reduce risk for that scenario. An appendix to the Facility Security Plan should contain the scenario(s) evaluated, the results of the evaluation, and the mitigation measures chosen.

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

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

Table 4: Vulnerability & Consequence Matrix

		Total Vulnerability Score (Table 3)		
		2	**3-4**	**5-6**
Consequence Level (Table 2)	3	**Consider**	**Mitigate**	**Mitigate**
	2	**Document**	**Consider**	**Mitigate**
	1	**Document**	**Document**	**Consider**

STEP 5: IMPLEMENTATION METHODS

To determine which scenarios require mitigation methods, the Facility Security Officer or company official may find it beneficial to use the Table 5 provided below. The facility or company can record the scenarios considered, the consequence level (Table 2), the score for each element of vulnerability (Table 3), the total vulnerability score, and the mitigation category (Table 4). The desire is to reduce the overall risk associated with the identified scenario. Note that generally, it is easier to reduce vulnerabilities than to reduce consequences or threats.

Table 5

MITIGATION DETERMINATION WORKSHEET					
Step 1	**Step 2**	**Step 3**			**Step 4**
Scenario/Description	**Consequence Level (Table 2)**	**Vulnerability Score (Table 3)**			**Mitigate, Consider, or Document (Table 4)**
		Accessibility +	Organic Security =	Total Score	
	Once a facility is categorized, the consequence level remains the same.				

To assist the Facility Security Officer or company official evaluate specific mitigation strategies (protective measures), it may be 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 Level (Table 2)**	**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. For those scenarios that scored as **consider** or **mitigate**, the facility or company 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 level remains the same as was determined in Table 2 for each scenario.
4. Re-evaluate the accessibility and organic security scores (Table 3) to see if the new mitigation strategy reduces the total vulnerability score for each scenario.
5. With the consequence level and new total vulnerability score, use Table 4 to determine the new mitigation categories.

A strategy may be deemed as effective if its implementation lowers the mitigation category (e.g., from **mitigate** to **consider** in Table 4). A strategy may be deemed as effective if the strategy will lower the overall vulnerability score when implemented by itself or with one or more other strategies. For example, for a facility with a consequence level of "2", if a mitigation strategy lowers the vulnerability score from "5-6" to "3-4", the mitigation category changes from **mitigate** to **consider** and the mitigation strategy is effective. For a facility with a consequence level of "3", the mitigation category would remain the same **(mitigate)** for a similar reduction in vulnerability score from "5-6" to "3-4".

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

As an example of a possible vulnerability mitigation measure, a facility or company may contract for additional security personnel to prevent unauthorized access during times of elevated threat levels. This measure would improve physical security and may reduce the total vulnerability score from a "3-4" to a "2". However this option is specific for this scenario and also carries a certain cost.

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

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 appropriate if there is a specific threat and/or an increase in MARSEC level. Mitigation strategies should ensure that the overall level of risk to the facility remains constant relative to the increase in threat.

Tables 7 and 8 provide an abbreviated example of how Tables 5 and 6 would be filled out for a bulk oil facility that is subject to 33 CFR 154 and receives vessels on international voyages. This example assumes that the facility has a fair deterrence capability with respect to organic security, however does not have a fenced perimeter to restrict access to the facility.

Table 7

MITIGATION DETERMINATION WORKSHEET					
Step 1	**Step 2**	**Step 3**			**Step 4**
Scenario/Description	**Consequence Level (Table 2)**	**Vulnerability Score (Table 3)**			**Mitigate, Consider, or Document (Table 4)**
		Accessibility + Organic = Total Security Score			
1. Gain unauthorized entry into the facility.	**2**	**3**	**2**	**5**	**Mitigate**
2. Externally attack the facility with a firearm.		**3**	**2**	**5**	**Mitigate**
3. Use the facility as a means of transferring people from a ship to a vehicle to illegally enter the U.S.		**3**	**2**	**5**	**Mitigate**
…		**…**	**…**	**…**	**…**

Table 8

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 Level (Table 2)**	**New Vulnerability Score (Table 3)**			**New Mitigation Results (Table 4)**
			Accessibility +	Organic =	Total Score	
1. Perimeter Fence that Restricts Access to the facility (meeting ASIS standards)	1. Intrude to the facility.	**2**	**2**	**2**	**4**	**Consider**
	2. Use the facility as a means of transferring people from a ship to a vehicle to illegally enter the U.S.	**2**	**2**	**2**	**4**	**Consider**
	…		…	…	…	…
2…	…		…	…	…	…