



## Port Security

"Seaports are difficult to secure due to their size, ease of accessibility by water and land, variety of potential targets, and close proximity to urban areas." Moreover, "The potential consequences of the risks created by these vulnerabilities are significant as the nation's economy relies on an expeditious flow of goods through seaports. A successful attack on a seaport could result in a dramatic slowdown in the supply system, with consequences in the billions of dollars."

\* In the GAO from May 17, 2005 entitled [Maritime Security: Enhancements Made, But Implementation and Sustainability Remain Key Challenges](#)\*



Port Security - Miami

The first step in improving the security of your facility is to implement an effective risk assessment program; doing so will ensure that your security dollars are expended in the most cost effective manner.

Understanding that security budgets are limited, CounterMeasures™ lists only those improvements that are suited to the business and security objectives you identify - and ranks recommendations accordingly. To help you prioritize your spending, CounterMeasures facilitates a cost-benefit analysis of each recommendation and identifies which are most beneficial per dollar spent to implement.

## What does CounterMeasures do?

CounterMeasures™ is a computer program that facilitates the conduction of a security assessment by facility owners, operators, or security officers. Facility personnel are prompted to enter information defining their facility and then the software will present the user with an appropriate list of regulations and security measures. As facility personnel identify which security measures they have in-place, the program will identify the security areas in which the facility has either compliance or security issue deficiencies. The program then allows the facility owner to browse from a list of possible security remediation efforts and sort them by effectiveness, price, or cost benefit analysis. The program generates a comprehensive set of reports on compliance, vulnerability, risk, and cost. As the Maritime Security (MARSEC) level changes, maritime organizations can quickly review the list of action items needed to comply with the changing MARSEC levels.





### **What are the benefits of using CounterMeasures?**

CounterMeasures™ Risk Assessment software accelerates and standardizes your organization's risk and vulnerability assessment program. Using interactive checklists with an easy-to-follow format, CounterMeasures™ enhances your self-assessment capability, eliminating the need for expensive security consultants. During the one-day training class included in the purchase price, you will learn how to use the software to conduct a security survey, analyze the results and print your [USCG Form 6025/6025A – Vulnerability and Security Measures Addendum](#).

### **What Regulations Does CounterMeasures Address?**

Our port security checklists are based on two sets of current Federal guidelines for seaport security: [Federal Register Part 105: Facility Security](#) and the U.S. Coast Guard's [Navigation Vessel Inspection Circular \(NVIC\) #11-02 change 1, Recommended Security Guidelines for Facilities](#). Both documents incorporate requirements and best practices for all three Maritime Security (MARSEC) levels established by the Coast Guard. Additionally, CounterMeasures™ automatically builds and populates Appendix A to Part 105 – Facility Vulnerability and Security Measures Summary ([Coast Guard Form CG-6025/6025A](#))

Sections addressing [Part 104: Vessel Security](#) and [Part 106: Outer Continental Shelf \(OCS\) Facility Security](#) are currently under development for inclusion in the seaport module.

### **Port Security References**

[33 CFR 104 Vessel Security](#)

[33 CFR 105 Facility Security](#)

[33 CFR 106 Outer Continental Shelf Facility Security](#)

[Maritime Transportation Security Act of 2002](#)

[NVIC 11-02, Ch I, Recommended Security Guidelines for Facilities](#)

[USCG Form 6025/6025A - Vulnerability & Security Measures Addendum](#)

### **MARSEC LEVELS**

The Coast Guard has a three-tiered system of Maritime Security (MARSEC) levels consistent with the Department of Homeland Security's Homeland Security Advisory System (HSAS). MARSEC Levels are designed to provide a means to easily communicate pre-planned scalable responses to increased threat levels. The Commandant of the U.S. Coast Guard sets MARSEC levels that commensurate with the HSAS. Because of the unique nature of the maritime industry, the HSAS threat conditions and MARSEC levels will align closely, though they will not directly correlate.

MARSEC levels reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, critical assets and infrastructure located on or adjacent to waters under U.S. jurisdiction.

**MARSEC Level 1:** Minimum appropriate security measures shall be maintained at all times. MARSEC 1 generally applies during HSAS Threat Condition Green, Blue, or Yellow.

**MARSEC Level 2:** Appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident. MARSEC 2 generally corresponds to HSAS Threat Condition Orange.

**MARSEC Level 3:** Further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable, imminent, or has occurred, although it may not be possible to identify the specific target. MARSEC 3 generally corresponds to HSAS Threat Condition Red.

