U.S. Department of Transportation
United States Coast Guard

Commandant
U.S. Coast Guard

2100 2nd Street SW
Washington, DC 20593-0001
Staff Symbol: G-MP
Phone: 202-267-0388
FAX: 202-267-4700

COMDTPUB P16700.4
NVIC 11-02
13 January 2003

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 11-02

Subj: RECOMMENDED SECURITY GUIDELINES FOR FACILITIES

1. PURPOSE.

a. This Navigation and Vessel Inspection Circular (NVIC) provides guidance on developing security plans, procedures, and measures for facilities. Until final regulations regarding *facility* security are published, this Circular may be used as a benchmark to develop and implement security measures and activities in anticipation of evolving domestic and international security regimes.

b. This Circular is structured similar to the recently adopted International Ship and Port Facility Security (ISPS) Code. Enclosure (1), like Part A of the ISPS Code, provides definitions and general guidance to *facility* owners or *operators*. Enclosure (2), like Part B of the ISPS Code, provides detailed security measures. Enclosures (3) through (5) provide additional information concerning implementing security measures for *facilities*. *Facility* owners or *operators* should develop a comprehensive security program by adopting the guidance in this circular.

c. The recently enacted "Maritime Transportation Security Act (MTSA) of 2002 (Pub. L. 107-295)," when implemented by regulations, will require security measures for ports, facilities, and vessels. In addition, the International Maritime Organization (IMO) adopted new maritime security measures as amendments to the International Convention for the Safety of Life at Sea (SOLAS). These measures resulted in a new SOLAS Chapter XI-2, "Special Measures to Enhance Maritime Security," and the ISPS Code." The international requirements can be found as Appendix B to the Coast Guard's Notice of Meetings; Request for Comments, Document USCG-2002-14069-1, and can be read at http://dmses.dot.gov/docimages/p74/210107.pdf. Regulations will soon be developed to implement the requirements of MTSA and the SOLAS amendments.

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)

d. The MTSA defines *facility* as “any structure or *facility* of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the United States." This indicates the clear intent that Coast Guard maritime security regulations should be aligned with our broader authority under the Ports and Waterways Safety Act (33 U.S.C. §§ 1221 et seq.) related to any public or commercial structure located on or adjacent to the marine environment, rather than our traditional approach of focusing on installations and terminals that have accommodations for vessels.

e. Until rules have been published, this Circular is intended only for *facilities* located in, on, under, or adjacent to any waters subject to the jurisdiction of the United States that handle: Class 1 (explosive) materials or other dangerous cargoes regulated under 33 CFR Part 126; liquefied natural gas and liquefied hazardous gas regulated under 33 CFR Part 127; oil and hazardous materials in bulk regulated under 33 CFR Part 154; general cargo (e.g., bulk, break bulk, and containerized cargo) transported by vessels engaged in international service and subject to SOLAS; or passenger vessels certificated to carry more than 150 passengers.

f. This Circular also includes additional recommendations for those *facilities* that handle *certain dangerous cargos* (*CDC Facilities*), as defined in section 1.2 of enclosure (1). Those recommendations are identified in enclosure (2) to this Circular.

g. This Circular does not apply to passenger terminals regulated by 33 CFR 128, *facilities* owned or operated by the Department of Defense, or passenger ferry terminals that service ferries certificated to carry more than 500 passengers. Guidance for passenger ferry terminals that service ferries certificated to carry more than 500 passengers may be found in the policy letter issued on September 4, 2002 by the Assistant Commandant of Marine Safety, Security, and Environmental Protection.

h. *Facilities* are very diverse. Some may be extremely large *facilities* that handle many large vessels and transfer and/or store large quantities of hazardous materials in densely populated areas. Other *facilities* may be very small, handle few vessels, and transfer and/or store very little hazardous material, and are located in remote areas. In addition, *facilities* may have intermodal corridors (rails, highways, pipelines, etc.) that pass through them. Access control from these corridors to adjoining areas of a *facility* requires the same level of security as exterior boundaries to the *facility*. Due to the different threats and consequences of an attack at each *facility*, the types and extent of security measures used at each *facility* must be commensurate with the threats and potential consequences.

i. The Coast Guard strongly supports performance based standards and accepts alternatives. Therefore this Circular provides tools for assessing equivalent security measures that may be incorporated into the *facility*'s security plans.

j. Certain *facilities* may be of such national, economic, or military significance that additional measures beyond those described here may be necessary. Working together, the Captain of the Port (COTP) and the owner/operator should identify the additional measures necessary to safeguard such *facilities*.

2. ACTION.

a. COTPs shall give the guidance in this Circular the widest dissemination to *facility* owners and operators within their Area of Responsibility (AOR). More importantly, COTPs retain discretion to modify security measures and plans as the situation dictates. They should consider alternatives offered by the *facility* that would provide an equivalent level of security to that intended to be achieved by these guidelines. This Circular will be distributed by electronic means only. It is available on the World Wide Web at http://www.uscg.mil/hq/g-m/nvic/index.htm.

b. *Facility* owners and operators may use these guidelines in cooperation and consultation with the COTP, local Port Security Committees or Harbor Safety Committees, as appropriate, to conduct security assessments of their *facilities*.

c. While the guidance contained in this document may assist the industry, public, Coast Guard, and other Federal and state regulators in applying statutory and regulatory requirements, the guidance is not a substitute for applicable legal requirements; nor is it a regulation itself.

d. The guidelines are not intended to restrict the lawful exercise of COTP authority to mandate security measures through a COTP order, consistent with paragraph 4.b. below. These guidelines should be considered in supporting a COTP order or security zone, as appropriate.

e. The intent of this NVIC is to provide guidelines that will assist *facility* owners and operators with managing risks to their *facilities*. It is not the intent of these guidelines to promote unreasonable restriction of mariners' shore leave as defined in the Convention on Facilitation of International Maritime Traffic -1965[1]. This Convention, to which the U.S. is a Party, provides that foreign crews shall be allowed ashore by public authorities while the ship on which they arrive is in port, provided the formalities on arrival of the ship have been fulfilled and the public authorities have no reason to refuse permission to come ashore for reasons of public health, public safety, or public order. These guidelines are not intended to alter U.S. obligations under that Convention. Portions of these guidelines address *facility* owners' and operators' treatment of debarked mariners on their *facilities*.

f. *Facility* owners and operators are reminded that authorized entry of mariners into the United States is administered by cognizant Federal authorities executing Federal statutes. If a crewmember does not have the appropriate credentials to go ashore, (e.g. a valid visa), or does not pass the Immigration and Naturalization Service (INS) inspection at the first port of entry, the INS will issue a Detain on Board notice to the mariner(s) and master. Depending on the circumstances of the specific case, the Coast Guard and the INS may require an appropriate security plan to ensure the Detain on Board mariner(s) remains on board. All other mariners on board who have been cleared by INS are authorized shore leave.

3. DISCUSSION.

a. *Facilities*, including public and military sites, may be the object of those desiring to do harm to the interests of the United States. In January 2002, the Coast Guard held a public workshop to discuss security procedures, programs, and capabilities within the marine

[1] Annex 1; Section 1; Part A. Definitions: "Shore Leave. Permission for a crew member to be ashore during the ship's stay in port within such geographical or time limits, if any, as may be decided by the public authorities.

transportation system. COTPs engaged their local port stakeholders to address security at *facilities*. The Coast Guard, including the COTPs, met with *facility* owners, port authorities, municipal, state, and Federal agencies, the Harbor Safety Committees, trade groups, and industry leaders to address security concerns. These guidelines are the result of those meetings and are provided as a means of promoting industry best practices to advance our vital national security interests.

b. Owners and operators of *facilities* have the primary responsibility for ensuring the security of their *facilities*. These guidelines do not relieve the owners and operators of their legal responsibilities, but rather are a means to help them meet their responsibilities to provide a safe and secure venue for vessels, passengers, cargo and employees. These guidelines also ensure the consistency of security measures within each port and provide a common security baseline at *facilities* across the country.

c. The U.S. Coast Guard will communicate heightened levels of alert using Maritime Security levels (MARSEC) 1, 2, and 3 that align with the graduated color-coded Threat condition levels defined by the Homeland Security Advisory System (HSAS). *MARSEC* is the maritime sector's tool for communicating risk and in most cases will be linked to the HSAS. *MARSEC Level 1* generally corresponds to the lowest three levels of HSAS: Green (Low), Blue (Guarded), and Yellow (Elevated); *MARSEC Level 2* corresponds to HSAS Orange (High); and *MARSEC Level 3* corresponds to HSAS Red (Incident Imminent). Ports, *facilities* and vessels should develop and implement protective measures, to be reflected in their security plans, which increase as the MARSEC level increases to reduce the risk of a transportation security incident. MARSEC levels may be assigned for the entire nation, or they may be set for a particular geographic area, industrial sector, or operational activity.

d. Although the intent is to promote more uniform practices and procedures, the guidelines were also drafted with the understanding that the threat levels or particular circumstances will differ among various geographic areas or ports based upon the risks present. It should be noted that it is possible to shift from *MARSEC* 1 directly to *MARSEC* 3 without an intermediate shift to *MARSEC* 2. When necessary, COTPs should exercise discretion and flexibility in determining which of the guidelines are appropriate for a given threat level or the unique circumstances within their zone of responsibility. For example, the COTP may find it necessary to adjust a previous measure prescribed for *MARSEC* 2, as long as an adequate level of security can be assured. On the other hand, a COTP may find it necessary to adopt a *MARSEC* 2 measure in *MARSEC* 1 because of heightened concerns that do not necessarily require all of the measures prescribed for the higher *MARSEC Level*, but still warrant additional security measures.

4. OTHER CONSIDERATIONS.

a. Authority. The primary authority for issuing COTP orders regarding waterfront *facility* security is the Magnuson Act (50 U.S.C. §§ 191 et seq.) and its implementing regulations. COTP orders related to security may also be issued under the Ports and Waterways Safety Act (33 U.S.C. §§ 1221 et seq.). It is also noted that the recently enacted MTSA requires *facilities* to develop *Facility Security Plans*. Regulations to implement this act are being developed.

b. Threshold requirements for exercising COTP authority.

(1) When exercising authority under the Magnuson Act to issue a COTP order, the COTP must find that the action to be mandated is "necessary in order to secure such vessel from damage or injury or to prevent damage or injury to any vessel, or waterfront facility or water of the United States, or to secure the observance of rights and obligations of the United States." With respect to the establishment of a security zone, the authority would additionally extend to actions "necessary . . . to safeguard ports, harbors, or territories . . . of the United States." Simply put, there must be some articulable security threat that encompasses the vessel or facility subject to the order. The process for assessing the threat and selecting control measures must not be "arbitrary or capricious." Moreover, the requirements imposed by the order or security zone must be reasonable in scope and rationally related to safeguarding the vessel, harbor, port, or waterfront facility from the articulable security threat(s).

(2) A finding of necessity under this standard should be based on a careful consideration of the cumulative information available to the COTP. All relevant factors should be considered, including the potential target of the threat, any specific geographic or operating conditions that may make a target vulnerable, current intelligence or other threat information, the adequacy of voluntary security measures taken by the vessel, and symbolic factors such as periods of national or religious holidays. Each of these factors may not individually rise to the standard required, but collectively may be sufficient. A generalized threat or warning, reinforced by more specific and credible information related to possible attacks or unlawful acts against a specific type of facility or vessel, could meet the standard enunciated in the Magnuson Act and its implementing regulations.

c. Application to State Facility Operations. Magnuson Act authority can be exercised over waterfront *facilities* owned and operated by a state and by political subdivisions of a state. This may include a requirement that persons or vehicles be inspected prior to entering a *facility*. Care should be taken to avoid mandates that would directly compel enactment of state legislation or require the states, in their sovereign capacity, to use law enforcement personnel as a mechanism of enforcing Federal law against private individuals. For example, a COTP order that specifically requires local sheriffs or state police to conduct an activity on a waterfront *facility*, such as vehicle inspections, may violate constitutional principles of federalism. Issuing a similar order directly to a state owned waterfront *facility*, without mandating that state or local law enforcement personnel must conduct vehicle inspections, would, however, pass constitutional scrutiny.

d. Passenger and Vehicle Inspection. Authority exercised under the Magnuson Act cannot displace the constitutional protections U.S. citizens enjoy, including freedom from unreasonable searches and seizures. The purpose of the inspections, which are quick and limited, is to secure the vital government interest of protecting vessels, harbors, and waterfront *facilities* from destruction, loss, or injury from sabotage or other causes of a similar nature. Such inspections are intended to ensure that incendiary devices, explosives, or other items that pose a real danger of violence or a threat to security are not present. Inspections must be limited and no more intrusive than necessary to protect against the danger of sabotage or similar acts of destruction or violence. The inspection should, however, be reasonably effective to discover incendiary devices, weapons, explosives, and other implements of destruction. Inspection techniques include, but are not limited to, magnetometers, physically examining the person or objects

visually or through the use of trained animals, electronic devices, or a combination of methods. The inspections must be conducted for a purpose other than the gathering of evidence for criminal prosecutions. If evidence of criminal activity or contraband is inadvertently discovered during security inspections, it should be treated as a criminal act and the appropriate procedures for such act should be followed.

e. Public Notification. Conspicuous signs should be posted in public places that describe in general terms the current security measures being taken to ensure the security of the *facility* and persons. For example, when vehicle or personnel inspections are conducted, and when weapons are to be prohibited, the *facility* should post visible signs and make appropriate announcements to notify personnel of these policies. These signs and announcements should also clearly state that entering the *facility* is deemed valid consent to the inspection of vehicles, persons, articles and effects. Furthermore, it should be made clear that those failing to give such consent or refusing screening and inspection shall be denied admittance.

5. IMPLEMENTATION.

a. Enclosure (1) provides background information, definitions, and general guidance to *facility* owners and *operators* for developing a comprehensive security program.

b. Enclosure (2) provides detailed security measures that should be incorporated into a *facility security plan,* and that can be tailored to address the risk to a specific *facility*.

c. Enclosure (3) is a comprehensive sample audit checklist for *facilities* that transfer, store, or otherwise handle *certain dangerous cargo*. It may be used to perform baseline evaluations or periodic audits when modified to suit a specific *facility*.

d. Enclosure (4) is sample *Declaration of Security*. The *Declaration of Security* provides a means for ensuring that critical security concerns are properly addressed throughout a vessel's stay at the *facility*.

e. Enclosure (5) outlines procedures to evaluate and document security measures. It provides an alternative to the standards offered in enclosures (1) thru (3). It is a simplified risk-based security assessment tool, which can be used to refine and tailor security measures to specific *facilities* or situations where the measures in enclosure (2) are impracticable, or to assess the equivalency of alternative approaches. Owners or operators are encouraged to document the process and results of these assessments and to provide suggestions on how this assessment tool might be improved.

6. EFFECTIVE DATE. These guidelines are effective upon receipt and will remain in effect until revised or superseded. They may also be amended as necessary to align with future legislation or regulations.

PAUL J. PLUTA
Rear Admiral, U.S. Coast Guard
Assistant Commandant for Marine Safety, Security
and Environmental Protection

Encl: (1) General Security Guidelines for *Facilities*
(2) Detailed Security Guidelines for *Facilities*
(3) Sample *Facility* Security Audit Checklist
(4) Sample Declaration of Security
(5) Guidance on Assessing *Facility* Security Measures

**General Security Guidelines for *Facilities***

## 1.1 Introduction

This NVIC establishes guidelines for developing security plans and implementing security measures and procedures. It is intended only for *facilities* that handle: Class 1 (explosive) materials or other dangerous cargoes regulated under 33 CFR Part 126; liquefied natural gas and liquefied hazardous gas regulated under 33 CFR Part 127; oil and hazardous materials in bulk regulated under 33 CFR Part 154; general cargo (e.g., bulk, break bulk, and containerized cargo) transported by vessels engaged in international service; or passenger vessels certificated to carry more than 150 passengers. This Circular also includes additional recommendations for those *facilities* that handle *certain dangerous cargos* (*CDC Facilities*), as defined in section 1.2 of this enclosure. Those recommendations are identified in enclosure (2) to this Circular. This Circular does not apply to passenger terminals regulated by 33 CFR 128, passenger ferry terminals that service ferries certificated to carry more than 500 passengers, or *facilities* owned or operated by the Department of Defense.

This guidance is based on existing NVICs, best practices from industry standards, and the International Ship and Port Facility Security (ISPS) Code and related SOLAS amendments that were recently adopted by the International Maritime Organization (IMO).

These guidelines address the following four objectives: awareness, prevention, response, and consequence management. Facility personnel must continually be aware of their environment and the domain in which they are operating as the critical first step to prevent acts that threaten the security of *facilities*. Prevention measures are those that are designed to increase the difficulty of unauthorized access and prevent the introduction of prohibited weapons, incendiaries, or explosives. Facility personnel must be prepared to address any act that threatens the security of the *facility* or vessels moored thereto. Consequence management can be directly linked to the ability of a *facility* to appropriately and quickly respond in order to mitigate the consequences of an act that breaches the security of the *facility*.

In order to achieve these objectives, this Circular embodies a number of functional elements. These include, but are not limited to:

- Gathering and assessing information with respect to security threats and exchanging such information with appropriate stakeholders;
- Establishing and maintaining communication protocols for *facilities* and vessels;
- Deterring or preventing unauthorized access to *facilities*, their *restricted areas*, and vessels moored to the *facility*;
- Deterring or preventing the introduction of unauthorized weapons, incendiary devices, or explosives to *facilities*;
- Providing means for raising the alarm in reaction to security threats or *security incidents*;
- Developing *facility security plans* based upon security assessments;
- Conducting training, drills, and exercises to ensure familiarity with security plans and procedures; and

- Arranging for a timely response by law enforcement personnel, and others, to any incident.

## 1.2 Definitions

Note: All words or phrases that have been defined in these guidelines have been italicized throughout the document.

For the purpose of this Circular, unless expressly provided otherwise:

*Captain of the Port* (*COTP*) means the Coast Guard officer designated by the *Commandant* to command a *Captain of the Port* Zone as described in 33 CFR Part 3, or their authorized representative.

*Commandant* means the Commandant of the U.S. Coast Guard as described in 46 CFR 1.01-05.

*Certain Dangerous Cargo* (*CDC*) means any cargo that is a:

a. Division 1.1 or 1.2 explosives as defined in 49 CFR 173.50.
b. Division 1.5D blasting agents for which a permit is required under 49 CFR 176.415 or for which a permit is required as a condition of a Research and Special Programs Administration exemption.
c. Division 2.3 “poisonous gas”, as listed in 49 CFR 172.101, that is also a “material poisonous by inhalation” as defined in 49 CFR 171.8, and that is in a quantity in excess of 1 metric ton per vessel.
d. Division 5.1 oxidizing materials for which a permit is required under 49 CFR 176.415 or for which a permit is required as a condition of a Research and Special Programs Administration exemption.
e. A liquid material that has a primary or subsidiary classification of Division 6.1 “poisonous material” as listed in 49 CFR 172.101 that is also a “material poisonous by inhalation”, as defined in 49 CFR 171.8 or that is in a bulk packaging, or that is in a quantity in excess of 20 metric tons per vessel when not in a bulk packaging.
f. Class 7, “highway route controlled quantity” radioactive material or “fissile material, controlled shipment”, as defined in 49 CFR 173.403.
g. Bulk liquefied chlorine gas and bulk liquefied gas that is flammable and/or toxic and regulated under 46 CFR 154.7.
h. The following bulk liquids:
    (1) Acetone cyanohydrin
    (2) Allyl alcohol
    (3) Chlorosulfonic acid
    (4) Crotonaldehyde
    (5) Ethylene chlorohydrin
    (6) Ethylene dibromide
    (7) Methacrylonitrile
    (8) Oleum (fuming sulfuric acid)

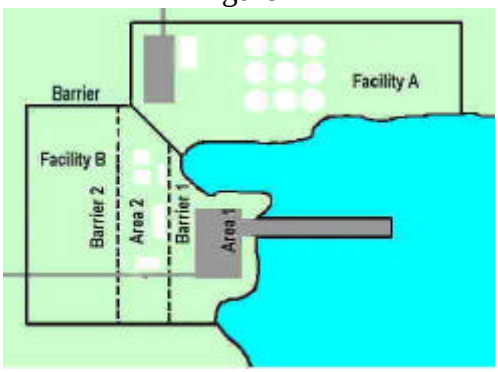
*Declaration of Security* (DOS) means an agreement to be executed between the responsible *Vessel Security Officer* and *Facility Security Officer,* and provides a means for ensuring that the critical security concerns are properly addressed and security will remain in place throughout the time a vessel is moored to the *facility*. Security for the *facility* is properly addressed by delineating the responsibilities for security arrangements and procedures between a vessel and the *facility*.

*Drills and Exercises* means frequent and detailed training conducted by the port *facility* to ensure that personnel are proficient in all assigned security duties, at all security levels, and to identify any security related deficiencies, which need to be addressed. Exercises are comprehensive training events that involve most of the items noted in Section 1.11 of this enclosure. Drills are more frequent but less comprehensive than exercises and are used to maintain a high level of security readiness.

*Facility* means all contiguous structures or *facilities* located in, on, under, or adjacent to any waters of the United States.

> **Note**: For the purposes of this NVIC the boundary of a *facility* extends from the ship/port interface, if applicable, to the inner-most continuous security perimeter enclosing (1) areas where cargo regulated under 33 CFR 126, 127 and 154 is stored, handled or processed, (2) all *restricted areas*, and (3) areas where passengers are received for vessels certificated to carry more than 150 passengers.
>
> When *restricted areas* or other essential areas are not adjacent or contiguous with the *facility*, the owner and/or *operator*, in consultation with the *COTP*, will determine the necessity of incorporating the non-contiguous area into the security plan.

Figure 1




Cargo Operations:

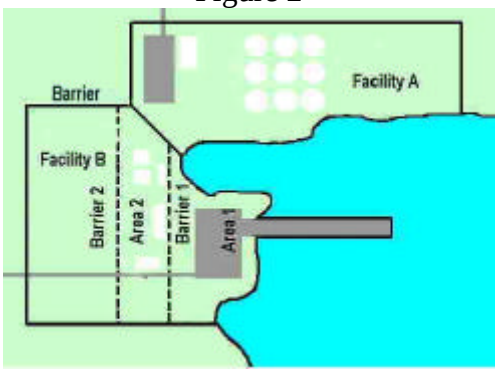
For facilities located adjacent to the waters of the United States that do not receive vessels (*Facility* A, Figure 1) but that handle, store, or transfer cargo regulated by 33 CFR 126, 127, or 154, the perimeter should surround those areas that handle, store, or transfer these cargoes.

For facilities that are adjacent to the waters of the United States that receive vessels (*Facility* B, Figure 1), the perimeter should extend, at a minimum, to Barrier 2 when cargo regulated under 33 CFR 126, 127, and 154 are handled, stored, or transferred in Area 2.

The perimeter may be limited to Barrier 1 (i.e. a smaller area) when Area 1 is the vessel/*facility* interface for vessels engaged in international service that do not handle cargo regulated under 33 CFR 126, 127 and 154.

Passenger Operations (*Facility* B, Figure 2):

Figure 2




When all activities essential to security are located in Area 1 for *facilities* that receive vessels certificated to carry more than 150 passengers, the perimeter may be limited to barrier 1. However, the perimeter should extend to Barrier 2 when activities that are essential to security, such as passenger or baggage screening, are conducted in Area 2.

*Facility Security Officer* (FSO) means the person appointed as responsible for the development, implementation, revision, and maintenance of the *Facility Security Plan*, and to serve as the liaison with the *Vessel Security Officers* and company security officers.

*Facility Security Plan (FSP)* means a plan developed to ensure the application of measures designed to protect the *facility* and vessels, their cargoes, and persons on board from the risks of a *security incident*.

*Facility Security Assessment* means an analysis that examines and evaluates possible threats, vulnerabilities, and existing protective measures, procedures and operations.

*Maritime Security (MARSEC) Level 1* means the level for which minimum appropriate protective measures must be maintained at all times..

*Maritime Security (MARSEC) Level 2* means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of a heightened risk of a transportation security incident.

*Maritime Security (MARSEC) Level 3* means the level for which further protective security measures shall be maintained for a limited period of time when a transportation security incident is probable or imminent, although it may not be possible to identify the specific target.

*Operator* means the person, company, governmental agency, or the representative of a company or governmental agency who maintains operational control over a *facility*.

*Restricted areas* means those portions of a *facility* identified by the owner/operator as being essential to the security of the operations, control, cargo or safety of a *facility*. Examples include, but are not limited to communications or control centers, utilities, pumping stations, tanks and piping systems, bulk and packaged hazardous cargo handling and storage areas, and Closed Circuit Television (CCTV) display rooms. As an alternative, the owner/operator may designate the entire *facility* a restricted area, as long as the entire *facility* is provided the appropriate level of security.

*Transportation Security Incident* means a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

*Vessel Security Officer (VSO)* means the person on board the vessel accountable to the master for the security of the vessel, including implementation and maintenance of the Vessel Security Plan and to serve as the liaison with the company security officer and the *Facility Security Officer*.

*Vessel facility interface* means the activities that occur when a vessel is directly and immediately affected by an action involving the movement of people, goods or the provisions of port services to or from the vessel.

### 1.3 Scope

This NVIC is intended for *facilities* that handle cargo that is subject to 33 CFR Parts 126, 127, and 154; receive vessel(s) that are certificated to carry more than 150 passengers (other than those required to comply with 33 CFR 128); or receive vessels on international voyages including vessels solely navigating the Great Lakes.

This NVIC also includes additional recommendations for those *facilities* that handle *certain dangerous cargos* (***CDC Facilities***), as defined in section 1.2. Those recommendations are identified in enclosure (2) to this NVIC.

*Facilities* that are not subject to 33 CFR Parts 126, 127, and 154; *facilities* that do not receive vessels certificated to carry more than 150 passengers; and *facilities* that do not receive vessels subject to SOLAS are not covered by this NVIC. The *facility* owner or operator has the primary authority for ensuring the security of the *facility*. Even modest security procedures can reduce vulnerability. Each *facility* operator is encouraged to implement a security program that incorporates appropriate preparation, prevention, and response activities should the need arise.

## 1.4 Maritime Security (MARSEC) Levels

*Maritime Security (MARSEC) Levels* were established to allow the Coast Guard to easily and clearly communicate the extent of threat present in a port. *MARSEC levels* also permit the *Captain of the Port* (*COTP*) and the port community to plan and pre-designate appropriate postures for each level of threat.

These levels are similar to the security levels used in 33 CFR Subchapter K, Security of Passenger Vessels, and the ones adopted by the International Maritime Organization (IMO) as the international maritime standard.

In March 2002, the President announced a national system for communicating threat levels, the Homeland Security Advisory System (HSAS). Homeland Security Presidential Directive (HSPD) – 3 defines a five-tiered system for setting threat levels. The Coast Guard is using a three-tiered system where *MARSEC* is generally linked to HSAS and serves as the maritime sector's tool for communicating risk. *MARSEC Level 1* corresponds to the lowest three levels of HSAS: Green (Low); Blue (Guarded); Yellow (Elevated); *MARSEC Level 2* to HSAS Orange (High); and *MARSEC Level 3* to HSAS Red (Incident Imminent).

## 1.5 USCG and *COTP* Responsibilities

While the intent of these guidelines is to present a broad-based approach to security, invariably there will be specific conditions or threats to the *facility* that will necessitate deviation from these guidelines. Accordingly, flexibility in these protective measures may be indicated for routine operations to address specific threats. Where practicable, *operators* should make the necessary preparatory steps to develop security measures for emerging threats. To assist with this effort, many of the security measures that were implemented in the immediate aftermath of the September 11, 2001 terrorist attack were considered for inclusion in these guidelines.

Through existing regulations in 33 CFR 6.16-3, the *COTP* retains the authority to issue written requirements for increased security measures to counter a specific threat. This authority may be used to carry out measures such as controlling the movement of vessels in the port, establishing security zones, or requiring vessel escorts. Accordingly, rather than issue general guidance for *facilities* to carry out these activities at the higher threat levels, these and other security measures may be implemented under the existing authority of the *COTP* to issue written orders based on specific threats to *facility* security. *COTP* orders would include limiting specific operations such as handling *certain dangerous cargoes*, until the order is complied with.

Similarly, other Federal agencies, such as the U.S. Immigration and Naturalization Service (INS), retain the authority to restrict personnel movements. For that reason, this NVIC will not address cases that involve stowaways and Detain on Board (DOB) personnel procedures.

## 1.6 Equivalent Standards

These guidelines were developed to assist *facility* owners and *operators* in establishing appropriate protective measures that address security activities and objectives. To provide flexibility and promote innovation, the Coast Guard will consider alternatives to the standards in this NVIC provided the alternatives provide equivalent levels of security. Owners and *operators* may present the cognizant *COTP* with an equivalency to specific protective measure(s) using the methodology identified in enclosure (5).

*Facilities* meeting an industry standard that has been reviewed and accepted in writing by Commandant (G-MP) will be considered as providing appropriate levels of security and meeting the guidance in this NVIC. Industry standards may include, but are not limited to, those prepared by the American Waterways Operators or the Chemical Carriers Association. At this time no standard has been accepted. As standards are accepted, they will be posted on the Coast Guard web page for ready reference.

*Facility* owners and *operators* may seek to demonstrate that the specific protective measure(s) provided in enclosure (2) are not appropriate for a specific *facility* due to location, types of cargo handled, frequency of operations, etc. Enclosure (5) enables owners and *operators* to demonstrate that, because of reduced consequence and vulnerability, a *facility* does not need to mitigate (provide protective measures) a specific activity or objective.

## 1.7 Facility Security Officer

A *Facility Security Officer* should be designated for each *facility*. The duties of the *Facility Security Officer* may be delegated to other qualified personnel, but the *Facility Security Officer* is ultimately responsible for these duties. A person designated as the *Facility Security Officer* may act as the *Facility Security Officer* for one or more *facilities*, depending on the number or types of *facilities* a company operates. Where a person acts as the *Facility Security Officer* for more than one *facility*, it should be clearly identified which *facilities* this person is responsible for, and be acceptable to the *COTP* for the zone in which those *facilities* operate. The *Facility Security Officer* may be a collateral duty provided the person is fully capable to perform the duties and responsibilities required of the *Facility Security Officer*.

The duties and responsibilities of the *Facility Security Officer* should include, but are not limited to:

- Conducting an initial comprehensive security assessment of the *facility* in order to prepare a *Facility Security Plan*;
- Implementing and exercising the *Facility Security Plan*;
- Undertaking regular security inspections of the *facility* to ensure the continuation of appropriate security measures;
- Recommending and incorporating, as appropriate, modifications to the *Facility Security Plan* in order to correct deficiencies and to update the plan to take into account relevant changes to the *facility*;

- Enhancing security awareness and vigilance;
- Ensuring adequate training for personnel responsible for security of the *facility*;
- Reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the *facility*;
- Coordinating implementation of the *Facility Security Plan* with the master(s) or Vessel Security Officer(s) as appropriate;
- Coordinating with security services, as appropriate;
- Ensuring that standards for personnel responsible for security of the *facility* are met; and
- Arranging for a timely response by law enforcement personnel, and others, to any incident.

## 1.8 Facility Security Assessment

The *Facility Security Assessment* is an essential and integral part of the process for developing and amending the *Facility Security Plan*. In addition to periodic updates and reviews, the *Facility Security Assessment* provides the opportunity for the owners to monitor compliance with the *Facility Security Plan* and make amendments as necessary. The *Facility Security Officer* may delegate the assessment to a person(s) with skills to evaluate the security of a *facility* and carry out the *Facility Security Assessment*.

Prior to commencing a *Facility Security Assessment*, the *Facility Security Officer* should obtain current information on the assessed threat for the local area and should be knowledgeable about type of vessels calling on the *facility*. The person should identify and evaluate possible threats to key *facility* operations, assets and infrastructure, and the likelihood of their occurrence, in order to establish and prioritize security measures. Possible threats to key *facility* and vessel operations may include:

- Bombing;
- Sabotage;
- Unauthorized use;
- Smuggling;
- Cargo tampering;
- Stowaways; and
- Cyber tampering.

The *Facility Security Officer* should study previous reports on similar security requirements. When feasible, the *Facility Security Officer* should consult with appropriate port personnel and other *Facility Security Officers* on the methodology and aspects of the assessment.

The *Facility Security Officer* should examine access points, including rail access, roads, waterside, and gates, and evaluate their potential for use by unauthorized individuals who may cause a *Transportation Security Incidents*. This includes individuals with legitimate access as well as those who seek to obtain unauthorized entry.

The *Facility Security Assessment* should include an on-scene security assessment and evaluation of the *facility*, to include the following elements:

- The general layout of the *facility*;
- The location and function of each actual or potential access point to the *facility*;
- Existing protective measures including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control, and similar systems.
- Numerical strength, reliability, and security duties of the *facility*'s personnel;
- Security doors, barriers, and lighting.
- The location of areas which should have restricted access, such as control stations, communications centres, cargo storage areas, etc.;
- The emergency and stand-by equipment available to maintain essential services;
- Response procedures for fire or other emergency conditions;
- Existing security and safety equipment for protection of personnel and visitors;
- The level of supervision of the *facility*'s crew, vendors, repair technicians, dock workers, etc.;
- Existing agreements with private security companies providing *facility* security services at all *MARSEC levels*, including any security forces contracted by visiting vessels;
- Procedures for control of security keys and other access prevention systems;
- Cargo and vessel stores operations; and
- Response capability to incidents.

The *Facility Security Assessment* should be documented and retained by the *facility*. The *Facility Security Assessment* should be performed periodically, taking account of changing threats and/or significant changes in the *facility*.

## 1.9 Facility Security Plan

Each *facility operator* is encouraged to develop an effective security program that incorporates detailed preparation, prevention, and response activities for each threat level-along with identifying the organizations, or personnel responsible for carrying out those activities. The *facility* owner or *operator* should document the security program in the form of a written *Facility Security Plan*. The plan should address the discrepancies identified in the *facility* security assessment and consider the recommended measures appropriate to the *facility*'s consequence level.

At *MARSEC Level 1*, *facilities* should carry out the following activities to prevent or deter *transportation security incidents*:

- Assign adequate resources to perform the prescribed security duties;
- Monitor *restricted areas* to ensure that only authorized persons have access;
- Control access to the *facility*;

- Monitor or patrol the *facility*, including mooring area(s);
- Supervise the security of cargo and vessel stores; and
- Ensure that security communication is readily available.

At *MARSEC Level 2*, in addition to *MARSEC Level I* protective measures, *facilities* should consider additional protective measures (see enclosure 2).

At *MARSEC Level 3*, in addition to *MARSEC Level 1 and 2* protective measures, *facilities* should consider additional protective measures to increase surveillance while significantly restricting access, to immediately identify and respond to *transportation security incidents* (see enclosure 2).

The *Facility Security Plan* should be developed taking into account the guidance in this NVIC and the relevant provisions of the Port Security Plan. The plan should, at a minimum, consist of:

- Measures and/or equipment designed to prevent or deter the unauthorized carriage of weapons, dangerous substances, and devices intended for use against people, vessels, or ports.
- Identification of the *restricted areas* and measures and/or equipment for the prevention of unauthorized access to the *facility* and to *restricted areas* of the *facility*;
- Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the *facility* or the vessel/port interface;
- Procedures for evacuation in case of security threats or breaches of security;
- Duties of *facility* personnel assigned security responsibilities and of other *facility* personnel on security aspects;
- Procedures for auditing the security activities, procedures for training, exercises, and drills associated with the plan;
- Procedures for interfacing with port and vessel security activities;
- Procedures for the periodic review and updating of the plan;
- Procedures for reporting *transportation security incidents*;
- Procedures for summoning emergency, safety, or security personnel including: local fire and police departments, SWAT, bomb disposal units, divers, hospital and EMT services, etc.
- Identification of the *Facility Security Officer* including 24-hour contact details;
- Measures to ensure the security of the information contained in the plan;
- Measures designed to ensure effective security of cargo and the cargo handling equipment at the *facility*.
- Procedures for auditing the *facility* plan;
- Procedures for responding in case the ship security alert system of a ship at the *facility* has been activated; and
- Procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship including representatives of seafarers' welfare and labor organizations.

The *Facility Security Plan* may be combined with other safety management systems. The plan *may be* kept in an electronic format. In such a case, it should be protected from being deleted, destroyed, or overwritten. The plan should be protected from unauthorized access or disclosure and treated as confidential information.

The *Facility Security Plan* contains information that pertains to the prevention of security incidents, such as procedures for communication and coordination to reduce the risk of, or vulnerability to a transportation security incident. To be effective when acts result in a transportation security incident, the procedures detailed in the *Facility Security Plan* must be coordinated with incident response plans. Therefore, *Facility Security Officers* should be mindful of the need to ensure that relevant crisis and consequence management plans exist for possible and actual transportation security incidents, and that such plans are referenced in the *Facility Security Plan*. *Facility Security Officers* should consider updating response plans to account for responses under heightened security levels and for resource trade-offs between security and response plans.

Upon moving to or from *MARSEC Level*s 2 and 3, the *facility* should acknowledge to the Coast Guard Captain of the Port the attainment of a change in *MARSEC Level* as described by the applicable Port Security Plan. The *facility* should inform any vessel moored at or en route to the *facility* that the *facility* is implementing the appropriate measures and procedures as detailed in the *Facility Security Plan* for the assigned MARSEC level. The *facility* should report any difficulties in implementation of security procedures within the *facility* or on those vessels moored at or en route to the *facility*. In such cases, the *Facility Security Officer* and *Vessel Security Officer* should coordinate the appropriate actions. The *facility* owner or *operator's* authority in matters of *facility* security remains unchanged. Maintaining *facility* security is an ongoing task. Additional security measures should be implemented to counter increased risks when warranted.

## 1.10 Records

Records of the following activities addressed in the *Facility Security Plan* should be kept for at least two years:

- Training, drills, and exercises;
- Reports of *transportation security incidents*;
- Report of breaches of security;
- Changes in *MARSEC levels*;
- Maintenance, calibration, and testing of security equipment;
- Communications relating to the direct security of the *facility* such as specific threats to the *facility*; and
- Periodic review of the security assessment.

## 1.11 Periodic Training, Drills, and Exercises

Drills should be conducted every three months with exercises every 12 months to ensure the adequacy of the *Facility Security Plans* described by this Circular. These exercises may be

*facility* specific, or part of a cooperative exercise program with applicable *facility* and vessel security plans. Communications and notification procedures should be included in every drill or exercise. Training may include, but is not limited to, the following, as appropriate:

- Security administration;
- Relevant national and international conventions, codes, and recommendations;
- Relevant government legislation and regulations;
- Responsibilities and functions of other involved organizations;
- Risk, threat, and vulnerability assessments;
- Security assessments and inspections;
- Ship and port operations and conditions;
- Vessel and *facility* security measures;
- Emergency preparedness, response and contingency planning;
- Instruction techniques for security training and education, including measures and procedures;
- Handling sensitive security related information and security related communications;
- Knowledge of current security threats and patterns;
- Recognition and detection of weapons, dangerous substances, and devices;
- Recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to commit *transportation security incidents*;
- Techniques used to circumvent security measures;
- Security devices and systems, and their operational limitations;
- Methods of conducting audits, inspections, control, and monitoring;
- Methods of physical searches and non-intrusive inspections;
- Security drills and exercises, including drills and exercise with ships; and
- Assessment of security drills and exercises.

## 1.12 Declaration of Security

The *Declaration of Security (DOS)* provides a means for ensuring that critical security concerns are properly addressed and security will remain in place throughout a vessel's stay at the *facility* or during vessel/vessel interface. Security is properly addressed by delineating responsibilities for security arrangements and procedures between a vessel and *facility* or between vessels. This obligation is similar to the existing U.S. practice for vessel/*facility* or vessel/vessel oil transfer procedures. At *MARSEC Level* 1, vessels carrying *certain dangerous cargoes* should complete a *DOS* for every interface. At *MARSEC Level* 2 and 3, a *DOS* should be completed for all vessel/*facility* interfaces. The COTP may, after assessing the risk, require the use of the DOS in additional circumstances, based on the risk.

The *Declaration of Security* should be completed by:

- The master(s) or the *Vessel Security Officer(s)*; and/or
- The *Facility Security Officer* or a person designated in the security plan to act on behalf of the Security Officer.

The *Declaration of Security* should address the security requirements that could be shared between a *facility* and a vessel and should state the specific responsibilities of each. The *Facility Security Officer* should be familiar with NVIC 10-02, Security Guidelines for Vessels, to ensure that critical security responsibilities are properly delineated and remain in place while a vessel is moored at a *facility*. Both the *facility* and the vessel should keep a copy of the *Declaration of Security*. The *Declaration of Security* should be made available to the *COTP* or their representative upon request. Enclosure (4) provides an example of a *Declaration of Security*.

For *facilities* that frequently receive the same vessel, a *Declaration of Security* for each interface is not required if the vessel and *facility* enter into a written agreement that states the responsibility for each during the vessel/facility interface. These agreements should be included in the Vessel Security Plan and *Facility Security Plan.*

## Detailed Security Guidelines for *Facilities*

### 2.1. General:

2.1.1. This enclosure provides specific guidance on establishing protective measures that should be implemented by *facilities* to achieve the four objectives of awareness, prevention, response, and consequence management.

2.1.2. *Facilities* that are not subject to 33 CFR Parts 126, 127, and 154; *facilities* that do not receive vessels certificated to carry more than 150 passengers; and *facilities* that do not receive vessels subject to SOLAS are not be covered by this NVIC. The *facility* owner or *operator* has the primary authority for ensuring the security of the *facility*. Even modest security procedures can reduce vulnerability. Each *facility operator* is encouraged to implement a security program that incorporates appropriate preparation, prevention, and response activities should the need arise.

2.1.3 This enclosure is structured along the topics listed below and correspond to section 16 of Part B of the ISPS Code. Each section in this enclosure has numbered guidelines that apply as indicated in the text.

2.1. General
2.2. Organization and performance of *facility* security duties;
2.3. Access to the *facility*;
2.4. *Restricted areas* within the *facility*;
2.5. Handling of Cargo;
2.6. Delivery of ship's stores;
2.7. Handling of unaccompanied baggage; and
2.8. Monitoring the security of the *facility*.

2.1.4. *Facilities* that handle and/or store *Certain Dangerous Cargoes* only on a limited basis (e.g., once or twice a year)--and would be designated as a ***CDC Facility*** during these operations--are encouraged to address those security measures recommended for ***CDC Facilities*** during those operations. Similarly, *facilities* that handle and/or store cargoes subject to 33 CFR 126 or 154, receive vessel(s) that are certificated to carry more than 150 passengers; or receive vessels on international voyages only on a limited basis (e.g., once or twice a year) are encouraged to address those security measures recommended in this guidance during those operations.

### 2.2. Organization and performance of *facility* security duties

2.2.1. *Facilities* should incorporate relevant security elements into the duties and responsibilities of all security personnel. Such elements should include, but not be limited to those intended to:

2.2.1.1. Heighten awareness that includes observing and reporting malfunctioning security equipment, suspicious persons, objects, and activities during rounds.
2.2.1.2. Implement measures required by the Facility Security Plan.

2.2.2. *Facilities* may implement the following protective measures to enhance security measures through the use of security personnel at all levels.

2.2.2.1. Develop and implement procedures for summoning additional security personnel from outside the *facility*, including local police, fire, SWAT, or medical services.
2.2.2.2. Security personnel should review and exercise their security duties and responsibilities through drilling and training.
2.2.2.3. Provide security information to all security personnel that includes the security level and any specific threats.
2.2.2.4. ***CDC Facilities*** should develop procedures for security personnel to record or report their presence at key points during their patrols.

## 2.3 Access to the *facility*

2.3.1. *Facilities* may implement the following protective measures to prevent or deter unauthorized access to *facilities* and vessels moored to the *facility* for all *MARSEC Level*s.

2.3.1.1. Limit the number of access points to the *facility*.
2.3.1.2. Monitor or secure all access points to *facility*.
2.3.1.3. Identify vehicles, persons, bags, cargo, stores or other materials approved for entry into *facility*.
2.3.1.4. Deny access to any person refusing to submit to security verification at a point of access. Each person denied entry for refusing to submit to security verification should be identified and reported to appropriate authorities.
2.3.1.5. Provide methods of identification for all employees and visitors. (See para 2.3.4. & 2.3.5.)
2.3.1.6. Establish parking procedures and designate parking areas. (See para 2.3.6. and 2.3.7.)
2.3.1.7. Allow only authorized personnel to have access to vessels moored at a *facility*.
2.3.1.8. Pre-schedule arrivals of vessels and work conducted on the *facility* with the proper authority. (See para 2.3.8.)
2.3.1.9. Erect fences or other barriers to delineate a perimeter where natural barriers do not form a boundary. (See para 2.3.9.)
2.3.1.10. **CDC *Facilities*** should establish procedures for escorting visitors, contractors, vendors, and other non-*facility* employees to their destinations when necessary. (See Note 1.)

2.3.2. *Facilities* may implement the following protective measures to prevent or deter unauthorized access to *facilities* and vessels moored to the *facility* during heightened *MARSEC levels*.

2.3.2.1. Implement procedures for escorting visitors, contractors, vendors, and other non-*facility* employees to their destinations when necessary. See Note 2.
2.3.2.2. Search/inspect all vehicles, persons, bags, deliveries, articles, or packages entering *facility*.
2.3.2.3. Consider restricting access to the *facility* to authorized and essential personnel. (See Note 1.)

2.3.2.4. Only persons with official *facility* or vessel's business should be authorized to embark or disembark a vessel moored to the *facility*. (See Note 1.)

2.3.2.5 **CDC *Facilities*** security plans should include a Traffic Control Program for vehicles entering and exiting the *facility*.

2.3.3. It is recommended that *facilities* implement a pass or badge identification system to identify all personnel. Personnel entering a *facility* should possess and show a valid tamper–resistant photo identification card and bear the name of the issuing authority to gain *facility* access. Security personnel or other competent authorities should verify that the I.D. card matches the person presenting it. These procedures should be closely monitored and enforced to preserve the integrity of the inspection, control and monitoring processes and the security of the *facility*. Acceptable means of identification and the procedures to be followed should be specifically provided for in the *Facility Security Plan* or procedures. *Facilities* should refer to the clarification of regulations notice entitled "Maritime Identification Credentials" published in the Federal Register (67 FR 51082, August 7, 2002) for more information on which credentials are deemed acceptable to the Coast Guard.

2.3.4. Permanent employees should display a picture ID badge or card at all times when working within restricted areas.

2.3.5 Unless essential to provide a specific service to the vessel, vehicles should not park on wharfs or piers. To provide an unimpeded view for security personnel, designated parking should be away from wharves and piers, areas used for storage of hazardous cargoes, and other areas designated as essential to the security of the *facility*. Where possible, designated parking should be outside of fenced operational, cargo handling, and storage areas. Security personnel should control or monitor access to designated parking areas.

2.3.6 **CDC *Facilities*** should register privately owned vehicles and contractor vehicles that are allowed routine access to the *facility* at the security office. Records should be maintained that include matching personnel with permit number and motor vehicle identification. Temporary permits should be issued to vendors and visitors for parking in designated areas. Security personnel should conduct random checks of parking permits.

2.3.7. Procedures for vessel personnel (pilots, crewmembers, agents, contractors, vendors and passengers on freight vessels) to depart or arrive by way of the *facility* should be coordinated in advance with proper security personnel in accordance with the *Facility Security Plan*.

2.3.8. Fencing should be adequate to prevent unauthorized access to a *facility*. For example, this may be achieved by meeting recognized industry standards, such as fencing standards recommended by the American Society for Industrial Security (ASIS), Chain Link Fence Manufacturers Institute (CLFMI), American Society of Testing Materials (ASTM), or other recognized industry standards. In general, these standards recommend that a fence be a minimum of 7 feet high with an additional 1 foot top guard for a total minimum height of 8 feet.

Note 1: Arrangements should be provided to allow vessel crewmembers that are cleared for entry into the U. S. to go ashore and be escorted to/from *facility* entrances.

## 2.4 ***Restricted areas* within the *facility***

2.4.1. *Facilities* should establish *restricted areas* to control access to key areas.

2.4.2 All *restricted areas* should be clearly defined and marked indicating that an area has restricted access. Markings should be clearly visible to all personnel.

2.4.3 The following are recommended protective measures for all *MARSEC Level*s that *facilities* may implement to enhance security in *restricted areas*:

2.4.3.1. Limit the number of access points.
2.4.3.2. Monitor or secure access to *restricted areas*.
2.4.3.3. Erect fences or other barriers to delineate perimeter where natural barriers do not form a boundary. (See paragraph 3.3.10.)
2.4.3.4. Block entry through windows to *restricted areas* (e.g. install bars on windows).

2.4.4. The following are recommended protective measures for r*estricted areas* during heightened *MARSEC Levels*

2.4.4.1. Dedicate personnel to guarding or patrolling *restricted areas* (*MARSEC* 2).
2.4.4.2. Enhance security through continuously guarding or patrolling *restricted areas* (*MARSEC* 3).

2.4.5. The following are recommended protective measures for *restricted areas* during heightened *MARSEC Levels* for ***CDC Facilities.***

2.4.5.1. Provide security at access points or perform routine security patrols.
2.4.5.2. Limit access to *restricted areas* except for security and essential personnel.
2.4.5.3. Dedicate personnel to guarding or patrolling *restricted areas* (*MARSEC* 2).
2.4.5.4. Enhance security through continuously guarding or patrolling *restricted areas* (*MARSEC* 3).

## 2.5. Handling of Cargo

2.5.1. The security measures relating to cargo handling should:

2.5.1.1 Prevent tampering, and
2.5.1.2 Prevent cargo that is not meant for carriage from being accepted and stored within the *facility*.

2.5.2 *Facilities* may implement the following protective measures to safeguard cargo against security threats at all *MARSEC levels*.

2.5.2.1. Verify and inspect cargo, cargo transport units, and cargo storage areas.
2.5.2.2. Develop inventory control procedures. Once within the *facility* cargo should be capable of being identified as having been checked and accepted for loading onto a ship or for temporary storage in a restricted area while awaiting loading. It may be

appropriate to restrict the entry of cargo to the *facility* that does not have a confirmed date for loading.

2.5.2.3. Develop cargo movement and storage procedures. The procedures should address such operations as cargo handling, receiving and releasing cargo, designated storage locations, and coordination with inventory control procedures.

2.5.2.4. Designate restricted area(s) to perform inspections of cargo.

2.5.2.5. Release cargo only to the carrier specified in the delivery order unless a release authorizing delivery to another carrier is presented and verified.

2.5.2.6. Routine checking of cargo within the *facility* prior to, and during, cargo handling operations;

2.5.2.7. Checks to ensure that cargo entering the *facility* matches the delivery note or equivalent cargo documentation; and

2.5.2.8. Screening of vehicles.

2.5.3. *Facilities* may implement the following protective measures to safeguard cargo against security threats during heightened *MARSEC levels*.

2.5.3.1. Segregate inbound cargo, outbound cargo, and vessel stores.

2.5.3.2. Increase the frequency and intensity of visual and physical inspections.

2.5.3.3. Limit the number of locations where hazardous cargo can be stored.

2.5.3.4 ***CDC Facilities*** should release cargo only in the presence of the *Facility Security Officer* or a designated representative of the *facility security officer*.

2.5.4. Verification and inspection of cargo for the detection and identification of prohibited weapons, incendiary, or explosive devices may be accomplished by:

2.5.4.1. Visual and physical examination;

2.5.4.2. Using scanning/detection equipment, mechanical devices, or canines;

2.5.4.3. Coordinating with shipper or other responsible party through an established agreement and procedures. For example, development and implementation of a Trusted Shipper Program.

2.5.5. Cargo stored in open areas, palletized or stacked cargo in warehouse *facilities*, should be properly stacked and placed within, away from, and parallel to non-perimeter fences and walls, to ensure unimpeded views for security personnel.

Note 2: The physical security provided in this NVIC meets the standards identified in the U.S. Customs Service, “Customs - Trade Partnership Against Terrorism” (C-TPAT) program. The Coast Guard and U.S. Customs have worked closely to ensure consistency between C-TPAT program and this NVIC.

## 2.6. Delivery of Ship's Stores

2.6.1. The security measures relating to the delivery of ship's stores should:

2.6.1.1. Ensure checking of ship's stores and package integrity;

2.6.1.2. Prevent ship's stores from being accepted without inspection;

2.6.1.3. Prevent tampering;

2.6.1.4. Prevent ship's stores from being accepted unless ordered;
2.6.1.5. Ensure searching the delivery vehicle; and
2.6.1.6. Ensure escorting delivery vehicles within the *facility*.

2.6.2 The following guidance is provided on supervising the security of ship's stores to adequately identify and take preventive measures against security threats at all *MARSEC levels*.

2.6.2.1. Verify and inspect ship's stores, transport units, and storage areas.
2.6.2.2. Require advance notification as to composition of load, driver details and vehicle registration;
2.6.2.3. Designate restricted area(s) to perform inspections of stores.
2.6.2.4. Screening of delivery vehicles.
2.6.2.5. Checks to ensure that ship's stores entering the *facility* matches the delivery note or equivalent documentation; and
2.6.2.6. Develop inventory control procedures. Once within the *facility*, ship's stores should be capable of being identified as having been checked and accepted for loading onto a ship. or for temporary storage in a restricted area while awaiting loading. It may be appropriate to restrict the entry of ship's stores that do not have a confirmed date for loading.

2.6.3. The following guidance is provided on supervising the security of ship's stores to adequately identify and take preventive measures against security threats at heightened *MARSEC Levels*.

2.6.3.1. Increase the frequency and intensity of visual and physical inspections.
2.6.3.2. Limit the number of locations where ship's stores can be stored.
2.6.3.3. Prepare for restriction or suspension of accepting or delivering ship's stores within all or part of the *facility*.

2.6.4. Verification and inspection of store's for the detection and identification of prohibited weapons, incendiary, or explosive devices may be accomplished by:

2.6.4.1. Visual and physical examination;
2.6.4.2. Using scanning/detection equipment, mechanical devices, or canines;
2.6.4.3. Coordinating with shipper or other responsible party through an established agreement and procedures. For example, develop and implement a Trusted supplier program.
2.6.4.4. Escorting the delivery vehicle within the *facility*.

2.6.5. Ship's stores stored in open areas, palletized or stacked in warehouse *facilities*, should be properly stacked and placed within, away from, and parallel to non-perimeter fences and walls, to ensure unimpeded views for security personnel.

## 2.7. Handling of Unaccompanied Baggage

2.7.1. At all *MARSEC levels*, the *facility* should establish security measures to ensure that unaccompanied baggage (i.e. any baggage, including personal effects, which is not with the passenger or ship's crew at the point of inspection or search) is identified and screened or

searched up to and including 100 percent, before it is allowed in the *facility* and, depending on the storage arrangements, before it is transferred between the *facility* and the ship. Such baggage does not need to be subjected to screening by both the *facility* and the ship. Steps should be taken to ensure that unaccompanied baggage is handled securely after screening.

2.7.2. *Facilities* may implement the following protective measures to safeguard the *facility* from threats posed by unaccompanied baggage during heightened *MARSEC Levels*.

2.7.2.1. Ensure unaccompanied baggage is subject to more extensive screening, such as x-raying it from at least two different angles.
2.7.2.2. Prepare to restrict or suspend handling of unaccompanied baggage; and
2.7.2.3. Prepare to refuse to accept unaccompanied baggage at the *facility*.

## 2.8 Monitoring the security of the *facility*

2.8.1. The following is a list of protective measures that *facilities* may implement to monitor the security of the *facility* and vessels moored to the *facility* for all *MARSEC Levels*.

2.8.1.1. Continuously monitor *facility* by using alarms, CCTV, or random security patrols. Perform patrols at irregular intervals to avoid established routines. (See paragraph 3.3.11.)
2.8.1.2. Provide security, such as routine patrols and/or electronic surveillance, for unmanned vessels moored at *facility*.
2.8.1.3. Search waterfront areas for explosives or other dangerous devices prior to a vessel arrival at *facilities* or waterfronts that have been unmanned or unmonitored.

2.8.2. The following is a list of protective measures that *facilities* may implement to monitor the security of the *facility* and vessels moored to the *facility* during heightened *MARSEC Levels*.

2.8.2.1. Increase random security patrols.
2.8.2.2. Dedicate personnel to guarding or patrolling the *facility* and vessels moored at the *facility*.
2.8.2.3 Search waterfront areas for explosives or other dangerous devices prior to a vessel arrival at ***CDC Facilities*** or waterfronts that have been unmanned or un-monitored.

2.8.3. Monitoring a *facility* may be accomplished by using alarms; Closed Circuit Television (CCTV); motion detection sensors; and/or personnel such as security patrols; or combination of these measures. Sensors, when used as a means to secure an area, should activate an audible and visual alarm when an intrusion is detected. The alarm should sound in a place that is continuously staffed by personnel with security responsibilities. Immediate on scene response (immediate = ten minutes or less) capability to an alarm from an intrusion detection system or device is important if its use is to be effective. System should be tested monthly or in accordance with the manufacturer's recommendations.

2.8.4. The following areas should be illuminated from sunset to sunrise or during periods of low visibility. In some circumstances it may be allowable to forego lighting, but the circumstances must be addressed in the *facility* security plan and it must be shown that the absence of lighting will not adversely impact risk and include the alternative measures being used. It is understood

that undesirable shadowing will exist, and the total elimination of shadowing is not practical in all areas.

2.8.4.1. Access points
2.8.4.2. Perimeter;
2.8.4.3. Piers/Wharves
2.8.4.4. *Restricted areas*;
2.8.4.5. Designated parking areas; and
2.8.4.6. Water surrounding vessels and piers/wharves.

2.8.5. The following guidelines should be considered when installing security lighting:

2.8.5.1. *Facilities* should be illuminated to an acceptable industry standard, such as the Illuminating Engineering Society of North America (IESNA) industry standard or other recognized industry standards.
2.8.5.2. To provide better visibility, updated lighting technology should be used, such as high-pressure sodium, mercury vapor, or metal halide lighting.
2.8.5.3. Lighting should be directed downward, away from guards or offices, or navigable waterways and should produce high contrast with few shadows.
2.8.5.4. The primary system should consist of a series of lights arranged to illuminate a specific area continuously during the hours of darkness or low visibility. In some circumstances, it may be preferable to use such lighting systems only in response to an alarm or during specific operations.
2.8.5.5. Portable floodlights may be used to supplement the primary system.
2.8.5.6. Portable floodlights when used should have sufficient flexibility to permit examination of the barrier under observation and adjacent unlighted areas.
2.8.5.7. Controls, switches, and distribution panels for security lighting should be located in *restricted areas*.
2.8.5.8. ***CDC Facilities*** should provide a secondary power supply line(s) separated from the primary power line(s). The *facility* should have the ability to rapidly switch to the secondary power line(s) during power failures.

2.8.6. Illumination is recommended whenever possible, but equivalent measures such as motion detectors or intrusion alarms may be used to monitor areas at *facilities* where illumination of the perimeter is unpractical or impacts aids to navigation. These areas should be identified in the *Facility Security Plan*.

2.8.7 Security personnel should have the ability to promptly notify appropriate personnel and be promptly notified of threats or breaches of security. This includes the capability to receive threat level information as passed by the *COTP* in the manner prescribed in the Port Security Plan. It can be achieved through the use of security systems and communications systems that are:

2.8.7.1. Maintained and operable;
2.8.7.2 Readily available;
2.8.7.3. Able to communicate within the *facility* and vessel if need be; and
2.8.7.4. Able to monitor and relay essential information from a central point.

2.8.8. *Facilities* may implement the following protective measures to enhance the detection and reporting of threats through the use of security alarms and communications systems:

2.8.8.1. At each *facility* access point, provide a means of contacting police, security control, or an emergency operations center. (e.g., telephones, cell phones, and portable radios)
2.8.8.2 Provide a backup means of communications.
2.8.8.3 Routinely test communications systems.
2.8.8.4. ***CDC Facilities*** should provide an alternate or independent power source for security and communications systems.

# Sample Facility Security Audit Checklist for General and Detailed Guidelines

This assessment form is a tool to assist in verifying the implementation of security plans for *facilities*. Certain measures may not apply to every plan. The completed assessment should be protected from unauthorized access or disclosure.

| | |
|---|---|
| Name of Facility: | Address: |
| City: | State: |
| Type of Facility (circle type): CDC Facility Other Facility: | |
| Date:<br><br>Performed by: | |

| No. | Facility Security Plan | Yes | No | N/A |
|---|---|---|---|---|
| 1. | Does the Facility have a current *Facility Security Plan* (FSP)?<br>Plan dated _____ Last Updated/Reviewed _____ | | | |
| 2. | Does the FSP designate a *Facility Security Officer*, and describe the duties and responsibilities of this officer? | | | |
| 3. | Does the FSP provide for measures and equipment necessary to prevent weapons or other dangerous devices from being introduced to the *facility* or vessels moored thereto? | | | |
| 4. | Does the FSP establish measures for the prevention of unauthorized access to the *facility* and vessels moored thereto? | | | |
| 5. | Does the FSP provide for the evaluation of all persons responsible for any aspects of security before they are employed? | | | |
| 6. | Does the FSP describe exactly the security measures and procedures actually in force at the *facility*? | | | |
| 7. | Does the FSP include procedures for obtaining assistance and support of law enforcement, fire, Hazmat, and explosive ordnance disposal units from Federal, State or local agencies? | | | |
| 8. | Does the FSP include procedures to be taken in the event of:<br>1. A bomb/terrorist threat?<br>2. An actual explosion or detonation?<br>3. A fire at the *facility* or on a vessel moored to the *facility*?<br>4. Natural Disasters?<br>5. A hostage situation?<br>6. Civil Disturbance/Labor Dispute?<br>7. Hurricanes?<br>8. Emergency Evacuation Procedures? | | | |
| 9. | Does the FSP have sketch of *facility* with all access points, working areas, storage areas, and cargo storage areas labeled? | | | |
| 10. | Does the FSP contain procedures to contact employees to Report/Not-To-Report to work? | | | |
| 11. | Does the FSP have a mechanism for accounting for all personnel on the *facility*, including their names? | | | |
| 12. | Does the FSP have specific measures to be taken in times of heightened risk? | | | |

Notes:

| No. | Organization and Performance of Facility Security Duties | Yes | No | N/A |
|---|---|---|---|---|
| 1. | Is the present security force strength and composition commensurate with the degree of security protection described in the *Facility Security Plan* (FSP)? | | | |
| 2. | Is a background check performed prior to hire and at least every five years thereafter for every employee who has a role in the *Facility Security Plan* or who has access to *restricted areas*? | | | |
| 3. | Are all security posts, fixed and mobile, provided with security force orders? | | | |
| 4. | Are security forces orders reviewed by the Security Officer for currency at least monthly? | | | |
| 5. | Are all security personnel required to wear uniforms that are complete, distinct, and authoritative? | | | |
| 6. | Do security personnel make regular patrols including building, perimeter, and wharf checks? | | | |
| 7. | Do security patrols include all exterior access points and principal interior access points to the *facility*? | | | |
| 8. | Does the *facility* or local community maintain an organized and equipped Crisis Response Force? | | | |
| 9. | Have procedures been prearranged for additional security forces to be brought in during emergency or crisis situations? | | | |
| 10. | Has liaison been established with Port Security Committees, Local, State, and Federal Law Enforcement Agencies whereby early warning of threat situation will be provided? | | | |
| 11. | * * Do security force personnel record or report their presence at key points in the *facility* by means of portable watch clocks, general watch clock stations, or telephones? | | | |
| 12. | Are guard assignments, times and patrol routes varied at frequent intervals to avoid establishing routines? | | | |
| 13. | If national, state, or local standards or certification regimes are in place, does the *facility* security force meet or exceed those requirements? | | | |
| 14. | Are individual training records maintained for security force personnel? | | | |
| 15. | Do all security force personnel, who are required to carry firearms, receive training? | | | |
| 16. | Does the security force have sufficient, adequately equipped vehicles to maintain patrols, respond to alarms and emergencies and maintain supervision? | | | |
| 17. | Are security force vehicles equipped with signs conspicuously identifying the vehicle as a security police vehicle, emergency exterior overhead lights, and an electronic siren? | | | |
| 18. | Are all security force vehicles equipped with a spotlight? | | | |
| 19. | Are only law enforcement personnel and other approved individuals allowed to carry firearms? | | | |
| 20. | Are duties other than those related to security performed by security personnel? | | | |
| 21. | Does the *facility* provide for security force inspection of the security barrier, including clear zones, at least once per month? | | | |
| 22. | Are records of these inspections maintained and easily accessible? | | | |
| 23. | Are Intrusion Detection System (IDS) signals monitored at one central point, and can a security force response be initiated from that point? | | | |
| 24. | Are all perimeter barrier portals guarded or secured, and locked when they are not in use? | | | |

| No. | **Organization and Performance of Facility Security Duties (con't)** | Yes | No | N/A |
|---|---|---|---|---|
| 25. | Are security measures in effect to protect electrical power supplies and transmission *facilities*? | | | |
| 26. | Are security measures in effect to protect communication centers/equipment? | | | |
| 27. | Are deficiencies noted and are remedial actions promptly effected? | | | |
| 28. | If a body of water forms any part of the barrier, are additional security measures provided? | | | |
| 29. | Are repairs to lights and replacement of inoperative lamps affected immediately or in a reasonable time | | | |
| 30. | Does the *facility* have an effective after hours or weekend restricted area security check by the security force? | | | |
| 31. | Does the *facility* security force use a duress code for emergency situations? | | | |

* * Recommend for ***CDC Facilities***

Notes:

| No. | Access to the Facility | Yes | No | N/A |
|---|---|---|---|---|
| 1. | Does fencing adequately prevent unauthorized access to the *facility* and meet recognized industry standards for fencing as recommended by the American Society for Industrial Security (ASIS), Chain Link Fence Manufacturers Institute (CLFMI), American Society of Testing Materials (ASTM), or other recognized industry standards? | | | |
| 2. | Is masonry or brick walls inspected every three months to determine the effectiveness and to assess any repairs due to erosion and wear? | | | |
| 3. | If building walls, floors and roofs form a part of the barrier, are they complemented by another means of intrusion detection such as Closed Circuit Television (CCTV) or motion detection sensors? | | | |
| 4. | Do all perimeter fences and walls have an unobstructed zone of at least 10 feet on each side? | | | |
| 5. | Are the gates and/or other entrances in perimeter barriers kept to the minimum number required for safe and efficient operations? | | | |
| 6. | Do all gates provide protection equivalent to that provided by the barrier of which they are part? | | | |
| 7. | Is a pass or badge identification system used to identify all personnel? | | | |
| 8. | Are all permanently employed personnel required to display a picture ID badge or card at all times when working within *restricted areas*? | | | |
| 9. | Does the identification medium in use provide the desired degree of security? | | | |
| 10. | Are personnel who have not been issued a permanent pass or badge, treated as "visitors", and issued a visitors badge or pass? | | | |
| 11. | Do guards at access points compare badges to bearers upon entry? | | | |
| 12. | Is supervision of the personnel identification and control system adequate in all areas? | | | |
| 13. | Are badges and serial numbers recorded and controlled by rigid accountability procedures? | | | |
| 14. | Are lost badges replaced with badges bearing different serial numbers? | | | |
| 15. | Have procedures been established that provide for issuance of temporary badges for individuals who have forgotten their permanent badges? | | | |
| 16. | Are badges of such design and appearance as to enable guards, and other personnel to recognize quickly and positively the authorizations and limitations applicable to the bearer? | | | |
| 17. | Are procedures in existence to ensure the return of identification badges upon termination of employment or assignment? | | | |
| 18. | * * Have effective visitor escort procedures been established when necessary? | | | |
| 19. | * * Are procedures in place to escort vessel crewmembers cleared to enter the U. S. to be escorted to and from *facility* entrances? | | | |
| 20. | Are truck drivers, vendors, and other visitors not permitted in the general offices of any terminal other than as required to conduct their business, and only authorized personnel are permitted in warehouses? | | | |
| 21. | Are permanent records of visits maintained and easily accessible? | | | |
| 22. | Are random administrative inspections made of vehicles entering the *facility*? | | | |

| No. | Access to the Facility (con't) | Yes | No | N/A |
|---|---|---|---|---|
| 23. | * * Does the *facility* have a Traffic Control Program? | | | |
| 24. | * * Is access to parking areas supervised and restricted by a permit system for privately owned vehicles and contractor vehicles? | | | |
| 25. | * * Are parking permit records maintained that include matching personnel with permit number and motor vehicle identification? | | | |
| 26. | Are all vehicles required to be parked in designated parking areas? Are employees, vendors, and visitors going to/from the parking area required to pass through an area under the supervision of security personnel? | | | |
| 27. | Is parking for employees, dockworkers, and visitors at least 50 feet away from the dock/wharf/pier, and outside of fenced operational, cargo handling, and designated storage areas? | | | |
| 28. | * * Are all temporary parking permits issued to vendors and visitors for parking in designated areas? | | | |
| 29. | * * Do Security personnel conduct random checks of parking permits? | | | |
| 30. | Are openings such as culverts, tunnels, and manholes for sewers and utility access, and sidewalk elevators, which permit access to the *facility*, properly secured? | | | |

* * Recommend for ***CDC Facilities***

Notes:

| No. | ***Restricted areas* within the Facility** | Yes | No | N/A |
|---|---|---|---|---|
| 1. | Have areas of the *facility* been designated in writing by the *facility operator* as *restricted areas* as necessary | | | |
| 2. | Are the basic security measures for *restricted areas* in effect? | | | |
| 3. | Are all *restricted area* access points appropriately posted? | | | |
| 4. | Do all *restricted areas* have a clearly marked perimeter barrier? | | | |
| 5. | Do all *restricted areas* have a personnel identification and control system with all entrances/exits guarded, controlled, or secured with alarms? | | | |
| 6. | Are only those personnel whose duties require access to information or equipment allowed within *restricted areas*? | | | |
| 7. | Are persons whose duties do not require access required to remain under constant escort while in *restricted areas?* | | | |
| 8. | Do all *restricted areas* have a personnel identification and control system? | | | |
| 9. | * * Is security provided at access points of *restricted areas*? | | | |
| 10. | * * Does security personnel perform routine patrols of *restricted areas*? | | | |
| 11. | * * Are procedures in place for personnel dedicated to guard or patrol *restricted areas* at MARSEC Level 2? | | | |
| 12. | * * Are procedures in place to limit access of *restricted areas* to security and essential personnel? | | | |
| 13. | * * Are procedures in place to continuously guarded *restricted areas* at MARSEC Level 3? | | | |

* * Recommend for ***CDC Facilities***

Notes:

| No. | Handling of Cargo | Yes | No | N/A |
|---|---|---|---|---|
| 1. | Are there procedures in place for the screening of vehicles entering the *facility*? | | | |
| 2. | Are there procedures in place for the movement and storage of cargo? | | | |
| 3. | Are there procedures in place for inventory control? | | | |
| 4. | Are there procedures in place to prevent tampering with cargo? | | | |
| 5. | Are there *restricted areas* designated to the perform the inspection of cargo? | | | |
| 6. | Is cargo stored in open areas, and palletized or stacked cargo in warehouse *facilities*, properly stacked and placed within, away from, and parallel to non-perimeter fences and walls, to ensure unimpeded views for security personnel? | | | |
| 7. | Are Electronic Data Interface (EDI) information and delivery orders for cargo and containers checked for accuracy and verified before acceptance? | | | |
| 8. | Are accesses to areas where documentation is processed limited solely to authorized personnel, and shipping documents safeguarded from theft? Is cargo documentation closely guarded to avoid documentation fraud? | | | |
| 9. | Are *certain dangerous cargoes* adequately described on the documentation, and the weights and piece counts indicated? | | | |
| 10. | Does the *facility operator* physically or electronically maintain, and continuously update, an accurate list of all cargoes, and a location chart, of all cargo/containers on the *facility*? | | | |
| 11. | Are delivery and receiving operations segregated? | | | |
| 12. | Are security measures in effect to protect arms, ammunition and dangerous cargos? | | | |
| 13. | Do drivers entering the *facility* show identification and obtain gate passes to control and identify those authorized to pick up or deliver cargo? | | | |
| 14. | * * Is cargo only released to the carrier specified in the delivery order unless a release authorizing delivery to another carrier is presented and verified? | | | |
| 15. | Do personnel processing delivery orders verify the identity of the trucker and trucking company before releasing the shipment? | | | |
| 16. | Are delivery documents closely scrutinized? Are seal numbers on containers verified against documents, and seals checked for integrity before arrival, departure, or transfer? | | | |
| 17. | Is cargo moved directly from railcars or vessels to storage *facilities*, and directly from storage *facilities* to railcars and vessels? | | | |
| 18. | Are the master flow and drain valves, and other valves that would permit direct outward flow of a bulk liquid storage tanks contents to the surface securely locked in the closed position when in a non-operating or non-standby status? | | | |
| 19. | Are the starter controls on all bulk liquid transfer pumps locked in the “off” position, or located at a site accessible only to authorized personnel? | | | |
| 20. | Are the loading/unloading connections of pipelines, loading arms, or transfer hoses securely capped or blank-flanged when not in service or in standby service? | | | |
| 21. | Are security personnel kept aware of the location of *certain dangerous cargos*, and are measures taken to implement a higher standard of security for these cargos? | | | |

* * Recommend for ***CDC Facilities***

Notes:

| No. | Delivery of Ship's Stores | Yes | No | N/A |
|---|---|---|---|---|
| 1. | Do drivers entering the *facility* show identification and obtain gate passes to control and identify those authorized to deliver ship's stores? | | | |
| 2. | Are procedures in place to visual and/or physically inspect ship's stores? | | | |
| 3. | Are there procedures in place to prevent tampering with ship's stores? | | | |
| 4. | Are inspections of delivery vehicles performed prior to entry into the *facility*? | | | |
| 5. | Are *restricted areas* designated to perform inspections of ship's stores? | | | |
| 6. | Are escorts provided for delivery vehicles within the *facility*? | | | |
| 7. | Are ship's stores scheduled in advance of delivery and coordinated between the *facility* security officer and the vessel? | | | |
| 8. | Are unscheduled deliveries of ship's stores prevented from being accepted? | | | |
| 9. | Are ship's stores screened using scanning/detection equipment, mechanical devices, or canines? | | | |

Notes:

| No. | Handling of Unaccompanied Baggage | Yes | No | N/A |
|---|---|---|---|---|
| 1. | Is unaccompanied baggage identified, screened prior to entering the *facility* or before transferring between *facility* and ship? | | | |
| 2. | Is unaccompanied baggage or personal effects, import cargos, export cargos, and domestic cargoes segregated from other cargo in a secured area? | | | |
| 3. | Are procedures in place to restrict, suspend, or refuse to handle unaccompanied baggage? | | | |

Notes:

| No. | Monitoring the security of the *facility* | Yes | No | N/A |
|---|---|---|---|---|
| 1. | Does illumination of *facility* meet an acceptable industry standard, such as the Illuminating Engineering Society of North America (IESNA), or other another recognized industry standards. | | | |
| 2. | Is the perimeter of the installation illuminated? (Continuous or standby lighting is acceptable) | | | |
| 3. | Is the perimeter of all *restricted areas* illuminated? (Continuous or standby lighting is acceptable) | | | |
| 4. | Are all vehicle entrances illuminated? | | | |
| 5. | Are all pedestrian entrances illuminated? (Continuous lighting is required for all open pedestrian entrances. Standby lighting is acceptable for pedestrian entrances that are locked or otherwise not accessible until security personnel authorize entry.) | | | |
| 6. | Are all docks, piers, wharfs and other working areas illuminated in a manner not to interfere with navigation? (Continuous lighting is required when there is any activity in these areas as a safety precaution. However, during times of inactivity, standby lighting is acceptable.) | | | |
| 7. | Are all water approaches to dock, pier, or wharfs illuminated? (Continuous lighting is required when there is any activity in these areas. However, during times of inactivity, standby lighting is acceptable.) | | | |
| 8. | Are all open yards illuminated? (Continuous or standby lighting is acceptable) | | | |
| 9. | Are parking lots illuminated? | | | |
| 10. | Are all parking lots illuminated in a manner to prevent shadows and areas of poor illumination between vehicles, and is the illumination even throughout the lot? | | | |
| 11. | Is perimeter protective lighting arranged so that security force patrol personnel remain in comparative darkness? | | | |
| 12. | Does the *facility* have an emergency backup power source for its protective lighting system? | | | |
| 13. | Are there provisions for standby or emergency protective lighting? | | | |
| 14. | Is lighting provided from sunset to sunrise and during periods of low visibility? | | | |
| 15. | * * Are procedures in place to search waterfront areas for explosives or other dangerous devices prior to a vessel arrival at *facilities* or waterfronts that have been unmanned or un-monitored | | | |
| 16. | Are all sensor equipment, doors, drawers and removable panels secured with key locks or screws and equipped with tamper proof switches? | | | |
| 17. | Is there an alternate or independent power source available for use on the system in the event of power failure? | | | |
| 18. | Does the *facility* employ any Intrusion Detection Systems (IDS)? | | | |
| 19. | Is the IDS inspected and/or tested at least monthly? | | | |
| 20. | Does the *facility* security force have its own communications system with direct communications between a security control/communications center and each security unit? | | | |
| 21. | Is there an alternate means of communication available to the security force? | | | |
| 22. | * * Is there a secondary power supply line(s) separated from the primary power line(s) that provide the ability to rapidly switch to the secondary power line(s) during power failures? | | | |

| No. | Monitoring the security of the *facility* (con't) | Yes | No | N/A |
|---|---|---|---|---|
| 23. | Is there an alternate or independent power source for security and communications systems? | | | |
| 24. | Does the security communications center have adequate physical security? | | | |
| 25. | Is the communication system capable of transmitting instructions to all security forces simultaneously in a rapid or timely manner? | | | |
| 26. | Is all communications equipment properly maintained? | | | |

* * Recommend for ***CDC Facilities***

Notes:

# (Sample) Declaration of Security

| | |
|---|---|
| _____ (Name of Vessel) | _____ (Name of Vessel/ Facility) |
| _____ (IMO Number) | _____ (IMO Number) or (Location) |
| _____/_____ (Registry)/(Flag) | _____/_____ (Registry)/(Flag), if applicable |

This *Declaration of Security* is valid from _____ until _____, for the following activities: _____under Security Level _____.

The involved parties agree to the following security responsibilities:

| Activity | (Responsible party to initial blank) **Vessel** | **Vessel/ Facility** |
|---|---|---|
| 1. Communications established between the vessel and vessel/facility: | _____ | _____ |
| (a) Means of raising alarm agreed between vessel and vessel/facility. | _____ | _____ |
| (b) Vessel/facility report/communicate any noted security non-conformities and notify appropriate government agencies. | _____ | _____ |
| (c) Port specific security information passed to vessel and notification procedures established (Specifically who contacts local authorities, National Response Center, and Coast Guard). | _____ | _____ |
| 2. Responsibility for checking identification and screening of: | | |
| (a) Passengers, crew, hand carried items, and baggage. | _____ | _____ |
| (b) Vessel store's, cargo, and vehicles. | _____ | _____ |
| 3. Responsibility for searching the berth/pier directly surrounding the vessel. | _____ | _____ |
| 4. Responsibility for monitoring and/or performing security of water surrounding the vessel. | _____ | _____ |
| 5. Verification of increased MARSEC level and implementation of additional protective measures. | _____ | _____ |

The signatories to this agreement certify that security arrangements during the specified *interface* activities are in place and maintained.

Date of issue ……

| | |
|---|---|
| _____ (Signature of Master or *Vessel Security Officer*) | _____ (Signature of Master, *Facility Security Officer, or authorized designee*) |
| _____ Name and Title, *Vessel Security Officer* Contact information_____ _____ | _____ Name and Title, Master or *Facility Security Officer* Contact information_____ _____ |

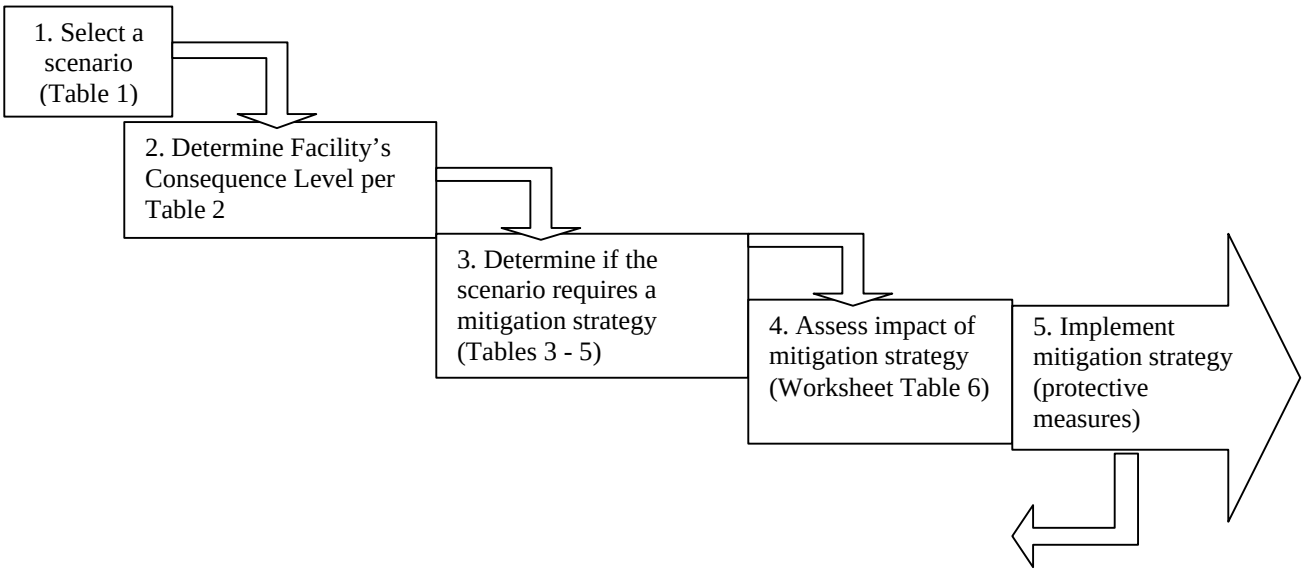
## Guidance on Assessing Facility Security Measures

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**<br>**(1) Are subject to 33 CFR Parts 126 and 154 (other than *certain dangerous cargoes*);**<br>**(2) Receive vessel(s) that are certificated to carry more than 150 passengers (other than those required to comply with 33 CFR 128); or**<br>**(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 = | Total Security 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 = | Total Security 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)** **Accessibility + Organic = Total Security Score** | | | **Mitigate, Consider, or Document (Table 4)** |
| **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 Security 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** | **4** | **Consider** |
| | … | | … | … | … | … |
| 2… | … | | … | … | … | … |