



**Table of Contents** ..... 1

**Vessel Data Sheet**..... 1

**Preface**

Plan, Purpose and Scope ..... 1

Record of Changes ..... 2

Distribution List of Controlled Copies..... 3

Vessel Security Assessment ..... 4

Information Provided to Vessel Captain ..... 4

Review by Authorities..... 5

Definitions ..... 5

**Section 1 - Security Organization of the Vessel**

1.1 Company Security Statement ..... 1

1.2 Captain’s Authority ..... 1

1.3 Security Organization and Individual Duties ..... 2

    1.3.1 Company Security Officer..... 3

    1.3.2 Vessel’s Captain..... 4

    1.3.3 Vessel Security Officer (VSO) ..... 5

    1.3.4 Vessel Personnel ..... 6

1.4 Crew Comfort and Privacy ..... 7

**Section 2 - Personnel Training**

2.1 Procedures ..... 1

2.2 Personnel Training Requirements ..... 1

    2.2.1 Personnel with Security-Related Duties ..... 1

    2.2.2 Other Vessel Personnel ..... 2



2.3 Training Reports and Records ..... 2

Figure 2-1 Training Frequency by Participant ..... 3

**Section 3 - Drills and Exercises**

3.1 Annual Exercise..... 1

3.2 Drills and Exercises ..... 1

3.3 Drill/Exercise Reports and Records ..... 2

**Section 4 - Plan Administration, Records and Documentation**

4.1 Security Records ..... 1

4.2 Distribution and Handling ..... 1

4.3 Security Sensitive Information ..... 2

4.4 Electronic Documents ..... 2

**Section 5 - Response to Change in MARSEC Level**

5.1 General ..... 1

5.1.1 Conformance to Port Level of Security..... 1

5.1.2 Failure to Conform to Port Level Security ..... 1

5.1.3 Vessel at Higher Security Level ..... 1

5.1.4 Acknowledgement and Briefings for Security Levels 2 and 3..... 1

5.1.5 Specific Security Measures to be Implemented Base upon the Security Level ..... 1

5.2 General Requirements for Security and Ensuring the Performance of Vessel Security ..... 2

5.2.1 General Security Requirements..... 2

**Section 6 –Procedure for Interfacing with Facilities and Other Vessels**

6.1 Communications with the Port and Facility ..... 1

6.2 Security Incident Reporting and Required Notifications ..... 1

6.2.1 Reporting to Government Contact Points ..... 1

6.2.2 Communicating With the Coast Guard ..... 1



**Table of Contents**

6.2.2.1 National Response Center ..... 1

6.2.2.2 Coast Guard Sector Command ..... 1

6.2.2.3 Maritime Security (MARSEC) Directives ..... 2

6.2.3 Reporting Changes in Security Levels ..... 2

6.2.4 Reporting Different MARSEC Security Levels ..... 2

6.2.5 Reporting Security Incidents ..... 3

6.2.6 Provisions to Maintain Critical Operations..... 3

6.2.7 Vessel Personnel ..... 4

6.2.8 Coordination of Visitors, Crew Changes and Shore Leave..... 4

6.3 Other Vessels..... 4

6.4 Interfacing with Ports, Facilities, Other Vessels or Offshore Installations ..... 4

    6.4.1 Interfacing with ports, a Facility or Another Vessel Not Subject to Security  
        Regulations or to which the Code Does Not Apply ..... 4

    6.4.2 Interfacing with fixed or floating platforms or a mobile drilling unit on location ..... 4

**Section 7 - Declaration of Security (DOS) ..... 1**

**Section 8 - Communications**

    8.1 Communication Systems and Equipment ..... 1

        8.1.1 Privately Owned Radio Devices..... 1

        8.1.2 Distress and Duress ..... 1

    8.2 Measures for Ensuring Security Communications ..... 1

        8.2.1 Security Measures ..... 1

    8.3 Mail Procedures..... 1

**Section 9 – Security Systems and Equipment Maintenance**

    9.1 Maintenance, Inspection, Testing and Calibration ..... 1

    9.2 Ship Security Alert System (SSAS) ..... 1

    9.3 Auto-Intrusion Detection Devices ..... 1



**Table of Contents**

9.4 Failure or Malfunction of Equipment or Systems ..... 1

9.5 Security Procedures for Dry Dock and Extended Maintenance Periods..... 1

**Section 10 - Security Measures for Access Control**

10.1 Access Control ..... 1

10.1.1 Vessel Access Points..... 1

10.1.2 Security Measures..... 1

10.1.3 Denial of Access ..... 1

10.1.4 Access Control Information ..... 1

Figure 10-1 Entry Sign ..... 1

10.1.5 Deck Watches ..... 2

10.1.6 Gangway / Main Access ..... 2

Figure 10-2 Security Instructions..... 4

10.1.7 Terminal / Port Access Procedures..... 4

10.1.8 TWIC Access Control Provisions ..... 5

10.1.9 Security Measures For Newly Hired Employees ..... 6

Figure 10-3 Vessel Access Procedures ..... 8

10.2 Controlling the Embarkation of Persons and their Property ..... 9

10.2.1 Security Measures..... 9

10.2.2 Screening Procedures..... 9

Figure 10-4 Access Control Listings ..... 10

10.2.3 Guidelines for Handling Unaccompanied Baggage ..... 11

Figure 10-5 Baggage Procedures..... 11

**Section 11-Security Measures for Restricted Areas**

11.1 Restricted and Vulnerable Areas ..... 1

11.1.1 Security Measures..... 1



**Table of Contents**

11.1.2 Security Procedures ..... 1

11.1.3 Master Keys ..... 1

Figure 11-1 Restricted Area Procedures..... 2

Figure 11-2 Restricted Area Listings ..... 2

**Section 12 - Security Measures for the Handling of Cargo**

12.1.1 Security Measures..... 1

12.1.2 Security Guidelines..... 1

Figure 12-1 Cargo Handling Procedures ..... 1

**Section 13 - Security Measures for Delivery of Vessel’s Stores and Bunkers**

13.1.1 Security Measures..... 1

13.1.2 Security Guidelines..... 1

Figure 13 Delivery of Stores and Bunkers Procedures ..... 1

**Section 14 - Security Measures for Monitoring**

14.1 Measures for Monitoring Deck and Areas Surrounding Vessel..... 1

14.1.1 Security Measures..... 1

14.1.2 Security Guidelines..... 1

Figure 14-1 Security Monitoring Procedures..... 1

**Section 15 - Security Incident Procedures**

15.1 Response to Security Incidents..... 1

15.2 Assessing Response to Security Incidents ..... 1

15.3 Incident Response Procedures ..... 1

15.3.1 Evacuation of the Vessel ..... 2

Figure 15-1 Port Evacuation..... 2

15.3.2 Bomb Threats..... 3

Figure 15-2 Bomb Threat Actions..... 4



Figure 15-3 Bomb Threat Checklist ..... 6

Figure 15-4 Letter and Package Bomb Recognition..... 7

**Section 16 – Audits and OMSA Alternative Security Plan Amendments**

16.1 Updates and Amendments..... 1

16.2 Periodic Reviews and Audits ..... 1

16.3 Evaluation of the Effectiveness of the OMSA ASP Plan..... 3

16.4 Revision of the ASP ..... 3

    16.4.1 Revision Intervals..... 3

    16.4.2 Revision Initiation ..... 3

    16.4.3 Revision Process ..... 4

**Section 17 – Vessel Security Assessment and Report ..... 1**

**Appendices**

- A - On-Scene Security Survey**
- B - Vessel Threat and Risk Assessment(s)**
- C – USCG/FBI Contact List \*\*Removed from VSP per Rev-1\*\***
- D - Towing Vessel/ Barge Addendum (Required for Towing Vessels)**
- E – Security Related Forms**
- F – Ship Security Alert System (if so equipped)**



## Preface

### Plan Purpose and Scope

This Offshore Marine Service Association (OMSA) Alternative Security Program (ASP) Vessel Security Plan (hereafter referred to as the OMSA ASP Plan, or Vessel Security Plan (VSP) has been developed to ensure that there are measures on board the vessel that are designed to protect persons, the environment, the cargo and the vessel itself from the risks of a security incident. This OMSA ASP Plan applies to the Master and crew.

The OMSA ASP PLAN has been prepared in accordance with:

- U.S. Coast Guard Regulations, 33 CFR Part 104

The Company has established this OMSA ASP Plan to assist the Company Security Officer (CSO), the Vessel Security Officer (VSO) and the crew to ensure the safety and security of the vessel, cargo and crew.

The purpose of the OMSA ASP Plan is to provide guidelines and procedures to prevent the following:

- Unauthorized access to the vessel and restricted areas on board;
- Introduction of unauthorized weapons or other dangerous devices on board;
- Introduction of contraband on board;
- Pilferage of cargo while in the care, custody and control of the vessel.

The Captain is ultimately responsible for the safety and security of the vessel. The Captain has the overriding authority and responsibility to make decisions with respect to the safety and security of the vessel and to request assistance from the Company and national or local authorities. This authority is further explained in Section 1.2 of this plan.







## Vessel Security Assessment

This OMSA ASP PLAN has been developed based upon a threat assessment, risk analysis, the Vessel Security Assessment (VSA) and On-Scene Survey conducted for this vessel. The VSA was conducted in accordance with the U.S. Coast Guard regulations, and is specifically tailored to domestic operations.

The Threat Assessment integral to this plan is based on a specific geographic region. The primary geographic region for this plan is the Gulf of Mexico, with a specific Threat Factors and Risk Assessment Report prepared, and included as Appendix B to this Plan. Additional Assessment Reports for other areas located in the United States such as East Coast, West Coast, Alaska, Hawaii, and Puerto Rico, are available for all plan holders and must be added to Appendix B whenever the vessel operates outside of the Gulf of Mexico operating area. The OMSA ASP Plan is valid for a vessel so long as the basic conditions which were in place at the time of the Vessel Security Assessment remain consistent.

*Any changes* in geographic operating area (i.e. from Gulf Coast to East Coast) will require the vessel operator to request a new threat assessment based upon the new operating area. The new threat assessment, provided by HudsonTrident, will be reviewed by the CSO and VSO, and entered into Appendix B of the OMSA ASP Plan, immediately in front of the base Threat Assessment for the Gulf of Mexico, which will always be stored in Appendix B (regardless of operating area). An annotation shall also be entered in the Record of Changes. Any change of cargo authorization (i.e. from oilfield cargo to general cargo) will necessitate the completion of a new VSA. The revised VSA will be entered into the appropriate tab of the OMSA ASP Plan and a change note made in the Record of Changes.

Changes to the plan, other than vessel data sheet information, must first be authorized by OMSA (who will consult with HudsonTrident and/or the U.S. Coast Guard, as necessary) *prior to any changes* made in the plan. Unauthorized changes to the OMSA ASP Plan will *automatically* invalidate the plan.

This OMSA ASP PLAN addresses all the vulnerabilities identified for this vessel during the VSA. The *Vessel Security Assessment and Report* is distributed, as authorized by the CSO, and is listed in the *Distribution List of Controlled Documents* found on the preceding page.

## Information Provided to Vessel Captain

The following information should be provided to the Captain by the Company:

- Parties responsible for appointing vessel board personnel, such as vessel management companies, manning agents, contractors, concessionaires;

**Preface**

- Parties responsible for deciding the employment of the vessel, including the time or bareboat charterer(s) or any other entity acting in such capacity; and
- In cases when the vessel is employed under the terms of a charter party, the contract details of those parties, including time or voyage charterers

**Review by Authorities**

This OMSA ASP Plan has been reviewed and approved by the U.S. Coast Guard in accordance with the Alternative Security Program authorized in U.S. Coast Guard regulations.

**Definitions**

**Coast Guard Sector Command (Sector)** created by merging traditional Groups, Marine Safety Offices (MSO) and Vessel Traffic Service (VTS) under one operational commander. The Sector Commander serves as the Captain of the Port (COTP), Federal Maritime Security Coordinator (FMSC) and unless otherwise delegated, the Officer in Charge Marine Inspections (OCMI), SAR Mission Coordinator (SMC) and Federal On-Scene Coordinator (FOSC) for a designated geographic region.

**Company Security Officer (CSO)** means the person designated by the Company for ensuring that a Vessel Security Assessment is carried out, that a OMSA ASP Plan is developed, submitted for approval, and thereafter implemented and maintained and for liaison with Port Facility Security Officers and the Vessel Security Officer.

**Declaration of Security (DoS)** means an agreement executed between the responsible Vessel and Facility Security Officer, or between Vessel Security Officers in the case of a vessel-to-vessel activity, that provides a means for ensuring that all shared security concerns are properly addressed and security will remain in place throughout the time a vessel is moored to the facility or for the duration of the vessel-to-vessel activity, respectively.

**Offshore Marine Service Association Alternative Security Program Plan (OMSA ASP Plan)** means a plan developed to ensure the application of measures on board the vessel designed to protect persons on board, cargo, cargo transport units, vessel's stores or the vessel from the risks of a security incident.

**Port Facility** is a location, as determined by the U.S. Coast Guard, where the "vessel-port interface" takes place. This includes areas such as anchorages, waiting berths and approaches from seaward, as appropriate.

**Preface**

**Port Facility Security Officer (PFSO)** means the person designated as responsible for the development, implementation, revision and maintenance of the Port Facility Security Plan and for liaison with the Vessel Security Officers and Company Security Officers.

**Screening** means a reasonable examination of persons, cargo, vehicles, or baggage for the protection of the vessel, its passengers and crew to ensure that dangerous substances and devices, or other items that pose a real danger of violence or a threat to security are not present.

**Maritime Security (MARSEC) Level** means the level set to reflect the prevailing threat environment to vessel and/or port environment. MARSEC Level is also known as Security Level.

**MARSEC Level 1** means the level for which minimum appropriate protective security measures shall be maintained at all times.

**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 heightened risk of a security incident.

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

**Secure Area** means the area on board the vessel over which the owner/operator has implemented security measures for access control in accordance with this Coast Guard approved security plan.

**Security Survey** means an inspection, check and/or audit to control and improve the mitigation strategy, protective measures and actions in the Vessel Security Plan.

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

**TWIC** means a valid, non-revoked transportation worker identification credential, as defined and explained in 49 CFR part 1572.

**TWIC Program** means those procedures and systems that the vessel must implement in order to assess and validate TWICs when maintaining access control.

**Vessel Security Assessment (VSA)** is a systematic and analytical risk-assessment process to consider the possibility that a security breach will affect personnel, the vessel, or her cargo. Based on this assessment, actions are identified to reduce the likelihood and



effects of a security breach. The OMSA ASP Plan is based on the results of the Vessel's Security Assessment.

**Vessel Security Officer (VSO)** is the person on board the vessel designated by the Company as responsible for the security of the vessel, including implementation and maintenance of the Vessel Security Plan and for liaison with the Company Security Officer and Port Facility Security Officers.

**Vessel/Port Interface** means the interactions that occur when a vessel is directly and immediately affected by actions involving the movement of persons, goods or the provisions of port services to or from the vessel.

**Unaccompanied Baggage** means baggage or parcels not arriving on board at the same time as their owner. This designation also includes packages carried on a "per-favor" basis, and baggage belonging to a crewmember that arrives on board at a different time from the crewmember; i.e. after being lost by an airline. Note: This does not include cargo with suitable documentation.



## **Section 6 – Procedures for Interfacing with Facilities and Other Vessels**

### **6.1 Communications with the Port and Facility**

Prior to entering a port or visiting an OCS facility, the Vessel Security Officer (VSO) shall establish communications with the Facility Security Officer (FSO) or offshore Facility Security Officer (FSO), if possible, in order to ensure maximum benefit from the security assets and procedures at the facility, or on the OCS facility.

During the vessels port call, or when servicing a facility on the Outer Continental Shelf (OCS), the Vessel Security Officer (VSO) will maintain communications with the FSO and appropriate port authority officials to fulfill the external relationship.

Communications with the FSO will be maintained with preference given to VHF radio and or telephone throughout the time the vessel is moored at the facility (using lines, ropes or dynamic positioning). The VSO will ensure that necessary communications equipment is available and that watch officers understand any special requirements for the port and/or facility. A communication plan will be established between the FSO and the VSO, including procedures for regular communication checks. The VSO shall notify the CSO if any problems are encountered with the organizations listed in the communication plan. The CSO will then take appropriate action necessary to remedy the situation, which may include notification of the applicable Coast Guard entities listed in Sections 6.2.2, below.

### **6.2 Security Incident Reporting and Required Notifications**

#### **6.2.1 Reporting to Government Contact Points**

Upon arrival at a port, the VSO will confirm, any security-reporting requirements in place for the port. During the port call, the VSO will ensure that all required reports are made.

#### **6.2.2 Communicating With the Coast Guard**

##### **6.2.2.1 National Response Center**

The Coast Guard National Response Center (NRC) is the central reporting location for the Coast Guard (800-424-8802), and shall be the method used to report any/all Transportation Security Incidents, see Section 6.2.5 for additional reporting details. Vessel operators may be most familiar with the NRC as the single official reporting location to the Coast Guard for oil spills or chemical releases.

##### **6.2.2.2 Coast Guard Sector Command**

Coast Guard field units combine Group Commands (law enforcement, search and rescue, aids to navigation) with Marine Safety Offices into Coast Guard Sector Commands. All reports concerning attainment of MARSEC Levels should



## **ALTERNATIVE SECURITY PROGRAM PLAN**

### **Section 6 – Procedures for Interfacing with Facilities and Other Vessels**

be directed to the Sector Command, whose current contact number can be accessed via the USCG Homeport web site at: <http://homeport.uscg.mil>. Vessels without internet capabilities should in concert with the CSO, complete a *Form-7, Port Communications Plan located in Appendix E* whenever operating in areas or locations where local USCG COTP numbers are not known, or readily available.

Vessels should contact Sector Commands to accomplish traditional Coast Guard Marine Safety functions.

#### **6.2.2.3 Maritime Security (MARSEC) Directives**

From time to time the Coast Guard may need to provide secure written communications with companies and vessels providing mandatory security measures. The Coast Guard will accomplish this through the use of MARSEC Directives.

When a MARSEC Directive is issued affected owners and operators need to go to their local Coast Guard Sector Command or cognizant District Commander to acquire a copy of the MARSEC Directive. Sectors and District Commanders will require owners or operators to prove that they are a person required by 49 CFR 1520.5(a) to restrict disclosure of and access to sensitive security information, and that under 49 CFR 1520.5(b), they have a need to know sensitive security information.

Each owner or operator of a vessel or facility to whom a MARSEC Directive applies is required to comply with the relevant instructions contained in a MARSEC Directive issued under this section within the time prescribed by that MARSEC Directive.

#### **6.2.3 Reporting Changes in Security Levels**

Upon receipt of a change in MARSEC Level from the Coast Guard, either through a local Broadcast Notice to Mariners, Maritime Security Directive, or as detailed in the Area Maritime Security (AMS) Plan, the VSO will, as soon as practicable; confirm to the local Coast Guard Sector, CSO, and FSO (if appropriate) of the attainment of measures or actions described in the vessel security plan and any other requirements imposed by the COTP that correspond with the MARSEC level being imposed by the change. Additionally, if in port, compliance with the higher MARSEC level is required to take place within 12 hours of notification.

#### **6.2.4 Reporting Different MARSEC Security Levels**

An owner or operator whose vessel is not in compliance with the requirements of this section must inform the USCG Sector and obtain approval prior to entering any



port, prior to interfacing with another vessel or with a facility or to continuing operations.

### 6.2.5 Reporting Security Incidents

Each breach of security, unlawful act or threat of an unlawful act against the vessel or persons aboard should be reported as soon as possible. Incidents that occur within the jurisdiction of the United States should be reported to the National Response Center (800-424-8802, as per 33CFR101.305), the Coast Guard Sector Command and the local Law Enforcement Authorities by the vessel operator or the CSO. Initial reports should be made as quickly as possible. After the vessel has transmitted an initial report, follow-up reports should be submitted at regular intervals to appropriate entities to keep them apprised of current events and developments. The *Incident Reporting Log* or a company substitute contained in Appendix E shall be utilized to document the incident. After an incident, Company management, the CSO and VSO will evaluate the effectiveness of the plan in accordance with *Section 16* of this plan. Reports must include, to the extent known:

- Vessel Name;
- Flag;
- Captain's Name;
- Name of Facility/Terminal (if moored);
- Incident Date, Time and Place;
- Incident Description;
- Number of Alleged Offenders;
- Description of any prohibited weapon, incendiary or explosive involved;
- Description of the way in which any prohibited weapon, incendiary device or explosive involved was concealed and used;
- Method used to introduce any prohibited weapon, incendiary device or explosive into or onto the vessel;
- Description of how security was breached; and
- Statement of measures taken or to be taken to prevent similar incidents.

### 6.2.6 Provisions to Maintain Critical Operations

The VSO should identify any operations critical to the vessel that may be affected by security measures. These operations should be brought to the attention of the FSO.



### **6.2.7 Vessel Personnel**

Any time the vessel's Security Level is changed, the VSO will ensure that the entire crew is made aware of this change.

### **6.2.8 Coordination of Visitors, Crew Changes and Shore Leave**

Prior to the vessel's arrival at a port or as soon thereafter as possible, the CSO should coordinate all expected visitors and crew changes with the VSO. Upon the vessel's arrival at the facility, the VSO should inform the FSO of all expected visitors and crew changes.

## **6.3 Other Vessels**

Any interaction with other vessels that affect the vessel's security should be coordinated between the VSO and the other vessel's VSO. The two VSO's should exchange contact information, their vessel's current Security Level, and any ongoing or planned critical operations.

## **6.4 Interfacing with Ports, Facilities, Other Vessels or Offshore Installations**

### **6.4.1 Interfacing with ports, a Facility or Another Vessel Not Subject to Security Regulations or to which the Code Does Not Apply**

Should the vessel be required to interface with a facility, another vessel, or call at a port not subject to U.S. security regulations, the VSO will assess any effect this may have on the vessel's security and direct appropriate additional security measures. These security measures will be reported to the CSO.

### **6.4.2 Interfacing with fixed or floating platforms or a mobile drilling unit on location**

Any interaction with fixed or floating platforms or a mobile drilling unit on location should be coordinated between the VSO and the Outer Continental Shelf (OCS) FSO or VSO, as appropriate. The VSO and FSO or drill ship VSO should exchange contact information, the current MARSEC Level each is operating under, and any ongoing or planned critical operations.

If the offshore facility is not subject to the Code and/or does not have a FSO, the CSO should be contacted, and the CSO will, together with the Master and VSO, assess any effect this may have on the vessel's security, and, if required, what additional security measures will have to be enforced.



This Appendix has been deleted.

Previous editions are now obsolete.