TABLE OF CONTENTS

Marsec, It's Name And Meaning

MARSEC is the term used for *Maritime Security*. Maritime Security is directed towards providing security for the United States by way of the waterways. The term *MARSEC* is derived from the first three letters of Maritime and the first three letters of Security. These letters were combined to form the word *MARSEC*.

MARSEC is primarily enforced by the **U**NITED **S**TATES **C**OAST **G**UARD (USCG) but is also enforced by the **D**EPARTMENT OF **H**OMELAND **S**ECURITY (DHS). The Coast Guard is a branch of the DHS and together they protect the United States from all enemies, both foreign and domestic that would wish to do harm to American civilians.

The Coast Guard's homeland security role includes:

- Protect ports, the flow of commerce, and the marine transportation system from terrorism.
- Maintain maritime border security against illegal drugs, illegal aliens, firearms, and weapons of mass destruction.
- Ensure that we (USCG) can rapidly deploy and resupply our military assets, both by keeping Coast Guard units at a high state of readiness, and by keeping marine transportation open for the transit assets and personnel from other branches of the armed forces.
- Protect against illegal fishing and indiscriminate destruction of living marine resources, prevention and response to oil and hazardous material spills--both accidental and intentional.
- Coordinate efforts and intelligence with federal, state, and local agencies.

Due to the nature of maritime security duties, it is necessary for all security officers to undergo training in MARSEC to be eligible for employment. This insures that every security

officer at Patriot Security EOC. is capable of performing the required duties as set forth by the U.S. Coast Guard in 33 CFR part 105.

Training and Supervision

All new Patriot Security EOC. officers are required to undergo training in Maritime Security before employment. The training is broken down into two different and distinct sections. Each section is designed to give the security officer the most efficient training possible in the most effective method available.

Section One deals with information that is relevant to all sites and is therefore called *General Information*. Section Two is information that is specific to each site and it is therefore called *Site Specific Information*. Section One is taught in the classroom whereas Section Two is taught on site. The sections are as follows:

Section One - General information

a. Knowledge of current security threats and patterns.
b. Recognition and detection of dangerous substances and devices.
c. Recognition of characteristics and behavioral patterns of persons who are likely to threaten security.
d. Techniques used to circumvent security measures.
e. The meaning and consequential requirements of the different MARSEC levels.
f. Crowd management and control techniques
g. Methods of physical screening of persons, personal effects, baggage, cargo and vessel stores.

Section Two - Site Specific Information

h. Security related communications.
i. Knowledge of emergency procedures and contingency plans.
j. Operation of security equipment and systems
k. Testing, calibrations and maintenance of security equipment and systems.
l. Inspection, control and monitoring techniques.
m. Relevant provisions of the Facility Security Plan

Terms and Acronyms[1]

As a security officer posted at a *MARSEC* facility you will hear terms and acronyms that you will need to be familiar with.

The list below are some of the most common acronyms you will most likely hear:

FSP	**F**acility **S**ecurity **P**lan	Plan designed for each facility to determine the security measures for each MARSEC Level.
FSO VSO CSO	**F**acility **S**ecurity **O**fficer **V**essel **S**ecurity **O**fficer **C**ompany **S**ecurity **O**fficer	This is the primary client contact for anything concerning *MARSEC*.
USCG	**U**nited **S**tates **C**oast **G**uard	Primary enforcer of *Maritime Security*.
DHS	**D**epartment of **H**omeland **S**ecurity	Government agency responsible for the safety and security of the United States.

Table 1.1
List of Common Acronyms

The list below are some of the most common terms you are most likely to hear:

Term	Meaning
Screening	Searching
Vessel	Boat or Ship
Moored or Berthed	Docked
Wharf	Dock

Table 1.2
List of Common Terms

1 A word formed from the initial letters of a multi-word name, for example: **U**nited **S**tates **C**oast **G**uard = USCG.

PATRIOT SECURITY EOC

We will now take a closer look at the information contained in

***SECTION ONE – GENERAL INFORMATION*.**

Knowledge of Current Security Threats and Patterns

As the world in which we live grows ever more complicated, the modern day security officer must be ever vigilant in the pursuit to stay ahead of those that wish to do harm to the American working class and way of life.

It is imperative that the security officer keep up to date on the threats of unlawful persons and the patterns they employ to accomplish their lawless deeds.

THREATS

A few examples of threats can be found in List 1. This list in no way includes all the types of threats presented to the facilities under the protection of the security officer, but it does include the most common ones that the security officer needs to be aware of.

Terrorism	**Vigilantes**
Disgruntled Employees	**Activist**
Theft	**Drugs/Alcohol**
Vandalism	**Arson**

List 1
Example of Threats

Terrorism

Terrorist are basically broken down into two parts, Foreign and Domestic. Foreign terrorist are persons that perform terrorist acts against a country in which they are **not** a citizen whereas a domestic terrorist are persons that perform terrorist acts against a country in which they **are** a citizen.

An example of a foreign terrorist for the United States would be Usama bin Laden also spelled Osama bin Laden

(لادن بن أسامة), the leader of Al Qaeda. Usama was born in Riyadh, Saudi Arabia.

An example of a domestic terrorist for the United States would be Timothy McVeigh who blew up the Alfred P. Murrah Federal Building in Oklahoma City or Ted Kaczynski who was called the Unabomber.

These are domestic terrorist because they are United States citizens and committed terrorist acts against their own country.

Vigilantes

A vigilante is someone who takes enforcement of law or moral code into his or her own hands. For this reason the security officer must be aware of persons that could possibly attempt to do harm to a facility because they have a grievance against it. Activist often fall into this category because they attempt to damage equipment and property of facilities and companies.

Disgruntled Employees

A disgruntled employee is difficult to identify. For this reason the security officer must always be on the lookout for client employees that might be "less than happy" with their employer and might take actions to do them harm.

A few things to look out for are employees that talk to you about being passed over for a promotion or raise, having an idea that was theirs stolen by a superior. Any of these could be signs that an employee might be unstable. These encounters should be reported to the client.

Activist

Activist can be very uncomforting for the security officer. As mentioned in *vigilantes*, activist often attempt to disrupt operation of a facility by damaging equipment and property. Thy also often hold protest with the intent of disrupting the day-to-day operations of a facility. In the event of a protest the security officer should be ever vigilant in keep a close eye

on the protestors to ensure that none of them breach the secure perimeter.

Theft

An employee may feel that the company or facility "owes" them something and therefore decide that taking something of value from the company or facility is justified. It is estimated that two-thirds of thefts are committed by employees.

For this reason many facilities require "Gate Passes" before any employee is allowed to exit with company items or tools of any type, even if the employee claims they are theirs.

Drugs/Alcohol

The security officer should always be on the lookout for drug or alcohol use. This type of activity endangers not only the employee using the drugs but everyone around him or her.

If drug/alcohol use is suspected but not directly observed by the security officer, never assume such activity has occurred. If you smell marijuana or alcohol it is proper to report what you have observed but never claim the person is intoxicated. You only report what you **know**, not what you **suspect or think** is true.

Vandalism

Vandalism is the conspicuous defacement or destruction of a structure or symbol against the will of the owner or governing body. It can be done as an expression of contempt, creativity, or both. In many cases it is perpetrated by young adolescents who think it is "fun" to spray-paint items, brake windows, uproot flowers and the like.

Security personnel should always be alert for such activity and preventing it where possible by their presence. Once an activity is in progress it should be reported to law enforcement. The security officers responsibility is to observe and report, **not** apprehend.

Arson

Arson is the crime of setting a fire with intent to cause damage. It is a rare crime but never-the-less one that security personnel should be aware of. If a fire is reported or observed by security personnel, if it is still very small and you are trained in the proper use of a fire extinguisher you may attempt to extinguish the fire if it can be accomplished without any possibility of harm.

If you are not trained in the proper use of a fire extinguisher or the fire is large, evacuate the area and call 911. In any case of a fire your primary responsibility is to safely evacuate the area and protect lives over attempting to extinguish the fire.

PATTERNS

In List 2 below are a few examples of patterns that could be used to threaten security. Patterns are to imitate or mimic the design of something. Therefore for our purpose it means the means by which a person may attempt to obtain **S**ENSITIVE **S**ECURITY **I**NFORMATION (SSI). *Sensitive Security Information* is information that is used by security personnel to perform their security duties.

Disguise	**Loitering**
Taking Pictures	**Unusual Vehicle Activity**
Diversions	**Counterfeit ID's**

List 2
Examples of Patterns

Disguise

Disguise is a very effective tool used by those wishing to circumvent security measures and is very simple to accomplish.

A disguise is not only someone wearing a fake beard or mustache, it is also a person pretending to be someone they are not. In short, a disguise is a form of deception, which is to

intentionally distort the truth in order to mislead others. This is accomplished in many different ways but a few are listed below. These are only a guideline, there are many other ways disguises can be used to gain access. The general rule is, if it falls out of **G**eneral **O**perating **P**rocedures (GOP) extra steps should be taken to ensure security is maintained.

Pretending to be an Employee, Delivery Person, Taxi Driver or Visitor

Anyone arriving at your post requesting access to a facility must be properly handled according to the **F**acility **S**ecurity **P**lan (FSP).

If a person arrives and states they are a new employee, you should contact the proper client personnel to verify the person's statement. Once verified, the new employee can then be processed as normal.

The same rule applies if a person arrives and claims to be a delivery person or a Taxi driver. (Some delivery services are given special treatment, such as UPS or Fed-EX by the client and you should follow the clients wishes in such cases.) In nearly all cases you should call the client contact listed in your *Post Orders* provided by Patriot Security Ltd. to verify the persons status for access onto the property.

Loitering

Loitering is to stand idly or to stop numerous times. In most cases this is not a security threat but someone who is waiting on another person or resting before moving on. Security personnel however, cannot take anything for granted. Never assume that the person is simply waiting on someone, you should always be aware of everything within your sight.

It should be stressed again that the security officers main objective is to deter by their presence and ***observe and report***. When you notice someone loitering, simply keep them under observation and note any strange or odd behavior.

If you feel that this person is observing your security duties, make a note of their description and report it to the Patriot Security office for further direction. ***DO NOT APPROACH THE PERSON.***

Taking Pictures

It is illegal to take pictures of any facility under MARSEC supervision. With the ever growing technology of cell phones it is becoming more difficult to enforce this law.

If you notice anyone taking pictures with a camera you should report it to the **F**ACILITY **S**ECURITY **O**FFICER (FSO) immediately. If the FSO informs you that they have permission you have performed your duty of **observing and reporting.**

If the FSO was not aware of the person taking pictures, you should continue observation of the person taking pictures. You should make notes on the person's description and movements and approximately what they were taking pictures of. ***DO NOT APPROACH THE PERSON.***

Once the incident is over the information in your notebook should be placed in a Patriot Security EOC ***Incident Report***.

Unusual Vehicle Activity

Unusual Vehicle Activity can be as simple as observing the same vehicle passing back and forth in front of your security building several times in a short period of time. Or it could be observing a vehicle stopping short of your gate and turning around to leave.

In most cases it will simply be someone lost or looking for another company or facility. In any case, make a note of it in an *Incident Report*. Your report should include the make, model, color, number of persons in the vehicle and license plate number if possible as well as the time of the incident.

Diversions

Diversions can be easily implemented. A small grass fire, fender bender on the road, two people fighting, etc. All of

these could be designed to draw your attention away from your duties and thereby allowing someone to gain access onto the property without your knowledge.

Your duties are to **observe and report**. In the event that any situation arises that could possibly be a diversion, maintain your post and report the situation to the client and follow their direction.

Counterfeit ID's

Counterfeit ID's can be used to gain inappropriate access onto the property. In recent times **I**NDUSTRIAL **S**AFETY **T**RAINING **C**OUNCIL (ISTC) badges have been counterfeited to gain access by workers that are not legal to be employed in the United States. These could also be used by terrorist to gain access to the property.

When looking at an ID, look for any signs of alterations such as picture is not correct, dates have been changed, card not in the right format or on the correct material.

Recognition and Detection of Dangerous Substances and Devices

DANGEROUS SUBSTANCES

Dangerous substances fall under many different categories. Not only are dynamite, TNT, guns and knives dangerous but many common substances can be considered dangerous as well if used improperly. List 3 shows a few of the common substances that could be considered dangerous if used improperly.

Gasoline or Diesel	**Welding Tanks**
Chlorine	**Ammonia**
Butane	**Propane**

List 3
Dangerous Common Substances

Gasoline or Diesel

Gasoline is a common component that is used to make what is commonly referred to as a "gas bomb" or "Molotov

cocktail." These combustible devices are simple to make and very effective when used as a device for arson.

Under no circumstances is anyone with such a device allowed onto the premises of any facility under *MARSEC* supervision. These devises have only one purpose, to cause havoc and destruction.

Welding Tanks

Welding tanks are generally made up of both oxygen tanks and acetylene

Chlorine & Ammonia

Chlorine & Ammonia are common everyday cleaning chemicals. Therefore if you were to screen (search) a cleaning crews vehicle and these items were present, you wouldn't think anything about. In other words, it's something you would expect to find in a cleaning crews vehicle. However, if it were in any other vehicle you should consider it uncommon and a security risk. Why? Because when these two chemicals are mixed together, they form a toxic gas.

Butane & Propane

Both butane and propane are explosive gases and should be treated as such. Many people use propane gas for their barbeque grill and when it is empty they take it to be refilled or exchanged. For this reason it is possible to find this item in an individuals vehicle.

No matter what the reason, or even if the container is empty, it cannot be allowed onto the property. It should be considered a security threat. It doesn't necessarily mean the owner of the container has any intention of doing anything improper with it. It must be confiscated until the person leaves the property.

DANGEROUS DEVICES

Dangerous devices come in many shapes, sizes and are made from many different materials. Almost anything can be made into a dangerous device.

List 4 below shows a few of the most common devices used in crimes and terrorist incidents.

Guns	**Knives**
Bombs	**Dirty Bombs**
Dynamite	**Letter Bombs**

List 4
Dangerous Devices

Guns & Knives

Guns and knives are two of the most popular items used in violent crimes. This in no way infers that guns and knives are dangerous just because they are *guns and knives*. These items are only dangerous if used improperly.

Billons of people use knives on a daily basis without causing harm to others. They use them to peal an apple or orange, to cut their steak or even simply spread butter on a piece of toast. But when used improperly, such as a weapon to kill someone, they become a dangerous device.

The same is true of guns. Contrary to popular opinion, no one has ever been shot by an empty gun. People have only been shot by a gun that they thought was empty, but that only happens because of the lack of respect and proper procedures for gun use.

Millions of people every day use guns for hunting, sports and self-protection. It is only when guns are used for unlawful purposes that they become a dangerous device.

Bombs

Bombs are explosive devises used to destroy people and property. They have no value other than to cause havoc and destruction. A bomb can be made to look like anything, a flashlight, camera, toy doll etc. For this reason, anything that is out of the ordinary should be considered suspicious. Never pick up anything that is laying around that could be a bomb.

Never use a cell phone, walkie-talkie or radio near an item you suspect could be a bomb. These radio waves could set

the explosive off. Remain at a safe distance from the item and ensure that no one else gets close to it.

Dirty Bombs

The term "dirty bomb" is most often used to refer to a **R**ADIOLOGICAL **D**ISPERSAL **D**EVICE (RDD), a radiological weapon which combines radioactive material with conventional explosives such as dynamite or **I**MPROVISED **E**XPLOSIVE **D**EVICE (IED). Though an RDD is designed to disperse radioactive material over a large area, the conventional explosive would likely have more immediate lethal effect than the radioactive material. Its purpose would presumably be to create psychological, not physical, harm through ignorance, mass panic, and terror.

Dynamite

Dynamite is most commonly used in construction to blast thru mountains and rock. If in the wrong hands it can be used to build a bomb (see Bombs above). The difference between a bomb and an explosive devise such as dynamite, is it's intended use.

Letter Bombs

Letter bombs, such as the types used by Ted Kaczynski (the Unabomber) are small explosives that explode when opened or picked up. The amount of explosive material is small because of the close proximity of the target.

In most cases, this does not effect the security officer because very seldom does a security officer deal with mail or parcel post material.

Recognition of Characteristics and Behavioral Patterns of Persons Who are Likely to Threaten Security

The ability to successfully recognize the behavioral patterns of those that are likely to threaten security is vital in your ability as a security officer to prevent security threats.

List 5 below list a few patterns that could be signs that a person is about to perform an illegal act.

Asking Security Related questions.	**Talking about the Government as if it is evil.**
Acting Nervous or Anxious	**Wearing Bulky Clothes**

List 5
Patterns of Persons Likely to Threaten Security

Asking Security Related Questions

Anyone asking you about the way you perform your security functions should be politely told "that information is privileged."

Talking About the Government as if it's Evil

We all have some dislikes about the way our government is ran and to some degree we all complain. This is not the type of situation I'm referring to.

The situation that security personnel should be concerned about is the kind where a person makes a statement about the American Government being the cause of the worlds problems or people that claim we deserved what we got on 9-11 because we are a corrupt nation.

Acting Nervous or Anxious

Acting Nervous or Anxious doesn't necessarily make a person a terrorist or criminal. They may have very good reasons for acting that way.

As mentioned before, if anything falls out of the **S**TANDARD **O**PERATING **P**ROCEDURES (SOP), you must call the client contact to verify the person's availability to enter the facility.

Wearing Bulky Clothes

A person wearing bulky clothing may just be wearing their style or they might be looking for something to steal. Security personnel should be aware of the people in their environment and the clothes they wear.

Techniques Used to Circumvent Security Measures

The techniques used to circumvent the security measures in place change on nearly a daily basis. Therefore it is very

important that the security officer remain up to date on the threats and techniques used by persons attempting to do harm to the facility under their control.

List 6 shows a few examples of techniques used to circumvent the security measures put in place to provide safety.

Digging Under Fences	**Cutting holes in Fences**
Climbing Over Fences	**Diversions**
Disguise	

List 6
Techniques Used to Circumvent Security Measures

Digging Under Fences

If you are making rounds and notice a hole under the fence that was not previously there, look at the dirt displacement to determine if it is a security breech or an animal digging under the fence. The dirt displacement should determine the necessary action needing to be taken.

When an animal digs a hole under fences the dirt is thrown in a random pattern directly behind the hole. When a human digs a hole the dirt is placed in a pile off to the side.

Cutting Holes in Fences

Holes in fences are a security violation that must be addressed immediately. These types of incidents should be reported to the **F**ACILITY **S**ECURITY **O**FFICER (FSO) as soon as possible.

Climbing Over Fences

If you observe anyone climbing over a fence it should be reported immediately. Nearly all fences at a MARSEC site are six feet high with either barbed wire, razor wire or both running across the top. This is a serious security breach and should be addressed immediately.

Diversions & Disguise

These were addressed earlier on pages 7 & 9, please refer to those pages.

Homeland Security

The Meaning and Consequential Requirements of the Different MARSEC Levels

Maritime Security is regulated by the **D**EPARTMENT OF **H**OMELAND **S**ECURITY (DHS) which the **U**NITED **S**TATES **C**OAST **G**UARD (USCG) is a branch of and the primary enforcers. The DHS has devised a color code system to advise the public of the seriousness of the threat to the United States. This code is called the **H**OMELAND **S**ECURITY **A**DVISORY **S**YSTEM (HSAS)and is pictured at right.

Maritime Security uses a different system but it is based on the HSAS system. The HSAS has five levels whereas the Maritime Security system has only three.

The chart below details the relationship between the two systems.

HSAS	MARSEC
SEVERE	**MARSEC 3**
HIGH	**MARSEC 2**
ELEVATED	**MARSEC 1**
GUARDED	
LOW	

The screening ratio is determined by the **F**ACILITY **S**ECURITY **P**LAN (FSP). Due to the sensitive nature of the screening ratio

per each MARSEC level, it is necessary that you be trained in that aspect of MARSEC on each individual site during phase two of your training.

Changing the MARSEC Level

When the **U**NITED **S**TATES **C**OAST **G**UARD (USCG) changes the MARSEC level, security personnel has 12 hours to implement the security changes needed to be in compliance with the new MARSEC level. AS a security officer you will be contacted by the **F**ACILITY **S**ECURITY **O**FFICER (FSO) to change the MARSEC level. The Coast Guard will ***NOT*** contact you.

It is very important that you understand that it is the **F**ACILITY **S**ECURITY **O**FFICER (FSO) that raises and lowers the MARSEC levels at the individual sites, ***NOT*** the **U**NITED **S**TATES **C**OAST **G**UARD (USCG).

When the MARSEC level is lowered, you will receive a call from the **F**ACILITY **S**ECURITY **O**FFICER (FSO) informing you that the MARSEC level is being lowered. After hanging up, you ***MUST*** call the **FSO** back to confirm that the MARSEC level is being lowered before you actually lower the current MARSEC procedures.

Crowd Management and Control Techniques

From time to time it is possible that you may be required to enforce crowd control. This is not a difficult task as long as you treat everyone with respect and ***NEVER*** lose your temper.

The primary duty of the security officer is to ensure that the area in their charge is safe and secure. This is primarily accomplished by your presence.

Follow these rules when presented with crowd control:

1. Keep the crowd calm
2. Always be polite but firm
3. Never raise your voice or scream at a person
4. Never act in an offensive manner.

NEVER MAKE ANY STATEMENTS TO THE NEWS MEDIA.

Be sympathetic with the crowds cause ***WITHOUT*** agreeing with it. Being sympathetic, again, without agreeing with the cause, can be a very powerful tool in keeping the crowd calm.

The general rule when presented with protestors is to neither agree or disagree with their cause, only be sympathetic with their predicament. This helps them feel that you understand them and thereby making them less anxious.

Crowd control also occurs when an emergency happens inside a facility. When this occurs you will be required to direct people to a safe staging point. A staging point is where people gather during an emergency until everyone can be accounted for.

You will need to make sure that no one leaves until the facility manager has given approval for them to leave.

Methods of Physical Screening of Persons, Personal Effects, Baggage, Cargo, and Vessel Stores

All facilities under MARSEC supervision are required to screen (search) vehicles that enter the property. Each site has it's own percentage that is unique to that site. The exact number of vehicles to be screened will depend on the **F**ACILITY **S**ECURITY **P**LAN (FSP) for that site and will be addressed when you are trained in section two, *Site Specific Information*.

As a Patriot Security Officer you will be required to screen vehicles. This is not a complicated task and only takes about five minutes to complete a through screening. When it is necessary to screen a vehicle, follow the guidelines below.

Areas to be screened

When screening make sure to screen the following areas:

- Inside the Vehicle
- Inside the Console
- Under the Hood
- Inside the Glove Box
- Under the Seat
- In the Trunk

- Inside Baggage
- Under the Vehicle

When screening, ***NEVER*** open any of the above mentioned items. It is the responsibility of the vehicle owner to open these items. For that reason, ask them to open the hood, trunk, glove box and console before they exit the vehicle.

Once they have done so they will need to go to the front of the vehicle and raise the hood. After they have raised the hood, ask them to stand by the drivers door. Never let anyone stand behind you or follow you as you screen the vehicle.

While looking under the hood special consideration should be given to ensure the hood does not fall on you. For this reason you should always keep one hand on the hood as you screen the engine compartment. Once you are done with the engine compartment, continue to the passenger compartment without closing the hood.

Once at the passenger compartment, look inside the glove box, which should have been opened before the driver exited the vehicle. Check for any items that are not allowed.

Look under the seat as well. When looking under the seat, do not place your hand under the seat to see if there is anything there. This is a safety violation. There could be a number of items that could either cut or stab the hand. To look under the seat, lean down and make a visual inspection.

Continue around the vehicle screening the rear seat compartment and trunk as well as any baggage they may have.

When you are finished screening, thank the vehicle owner for their patience and cooperation. At this point you should follow the rules and regulations of the specific facility you are securing concerning regular procedures for admittance.

SECTION TWO – SITE SPECIFIC INFORMATION.

In the second phase of your MARSEC training you will receive ***ON SITE*** training about the security procedures used at the site you are posted on.

Security Related Communication

Facilities use many different types of devices for communications, phones, cell phones, radios or walkie-talkies are just a few examples. You should make yourself familiar with how to use each of these means of communication.

Knowledge of Emergency Procedures and Contingency Plans

During an emergency, security personnel are required to assist in the evacuation and safety of the facility. Your duties are to ensure that the emergency procedures are followed and work as planed.

If there are any problems that you notice, report them to the **F**ACILITY **S**ECURITY **O**FFICER (FSO) so he can address those issues at a later date.

You will also most likely need to direct emergency personnel to the area of the emergency.

Operation of Security Equipment and Systems

There are a number of different security equipment and systems that the security officer may be required to operate at any facility. You should familiarize yourself with these items and how to properly use them.

Some sites use **C**LOSED **C**IRCUIT **T**ELEVISIONS (CCTV), electronic gates, golf carts, flashlights etc. on a daily basis. Once you are on a site you will be trained on these items if necessary.

Testing, Calibration and Maintenance of Security Equipment and Systems

On most sites the equipment belongs to the facility and should never be tampered with by the Patriot security officer. Therefore unless told, never calibrate or perform any type of maintenance on any equipment.

You may perform simple test from time to time on some equipment, such as opening and closing a gate, cycling thru cameras to ensure they all work etc.

Inspection, Control and Monitoring Techniques

Each facility will have it's own special techniques used to monitor and maintain a secure environment. As a security officer you will need to make yourself familiar with each facility and it's monitoring operations.

You will also need to be familiar with the inspection and control procedures used at each facility to enable you to perform your security duties.

Relevant Provisions of the Facility Security Plan

Each facility has a Facility Security Plan (FSP) that details the exact procedures required for their facility by the United Coast Guard (USCG) to ensure the security and safety of the United States and it's citizens.

As a security officer you will need to be familiar with the sections of the FSP as it relates to you. In most Facility Security Plans (FSP) the sections that deal with persons with security related duties, which the security officer is a part, is very small. In most cases it is less than ten pages.

These rules should be located in the Post Orders located on each site or they will be explained by a site supervisor, field supervisor or the client.

DICTIONARY

Berthed	To dock or tie a boat in a port.
Contingency Plan	A plan of action in the event the first plan doesn't work.
Department of Homeland Security	The government office responsible for the protection of the United States and it's citizens.
Facility Security Plan	The manual describing the rules and regulations required by a facility to comply with the Department of Homeland Security.
Homeland Security Advisory System	The system devised by the Department of Homeland Security to notify the public of the current threat level. See page 16 for a detailed explanation.
MARSEC	Maritime Security.
Moor	To tie a boat so that it stays in the same place.
Screen	Search
Staging Area	An area where people gather after an incident such as a fire or bomb threat.
United States Coast Guard	Primary enforcers of Maritime Security
Vessel	A large boat or a ship.
Wharf	An area like a wide wall built beside the edge of the sea or a river where ships can be tied and goods unloaded