1. Active Shooter. An active shooter incident is when one or more subjects participate in a shooting spree, random or systematic, with intent to continuously harm others. Active shooters are extremely dangerous and difficult because there is no criminal objective (e.g., robbery, hostage taking) involved other than mass murder. Often the shooter has no regard for his/her life and may be planning to die. The DHS defines an active shooter as an individual actively engaged in killing or attempting to kill people in a confined, populated space. In most cases, active shooters employ weapons that are concealable and fire on persons that they may or may not know. Past incidents include Columbine High School (Colorado) in April 1999, Virginia Tech University in April 2007, and Fort Hood (TX) in November 2009.

2. Individual responses. The arrival of security force members to an active shooter situation will more than likely occur sometime after the incident begins. Therefore, individuals must be mentally and physically prepared to deal with the situation to increase chances of survival. Familiarity with one's surroundings and continual vigilance will enhance situational awareness and increase individual alertness prior to an active shooter event. Practices include:

a. Be aware of the environment (e.g., potential dangers, locations of safe havens).

b. Be cognizant of objects that can provide cover and obstacles that may block exit.

c. Always identify the two nearest exits in any facility, in case of evacuation.

3. Evacuation. Should the individual decide the best chance of survival is to evacuate the threatened area, the following must be taken into consideration:

a. Remain calm.

b. Have an escape route and plan in mind.

c. Evacuate regardless of whether or not others agree to follow.

d. Leave belongings behind.

e. If possible, help others escape.

f. Attempt to prevent others from entering or returning to the threatened area.

g. Keep something between individuals and the shooter for cover.

h. Keep hands visible.

i. Follow the instructions of all security force members.

j. Provide any information on the situation to the security force members.

4. Remain in a secure position. Should evacuation not be possible nor the best option, the greatest chance of survival may be in the current location or a nearby, adjacent location that affords the best cover. Considerations include the following:

a. Remain calm.

b. If in an enclosure (e.g., office, rest room), secure doors, windows, and window blinds, and turn off lights.

c. If in a hallway, move immediately to an enclosure and secure it.

d. Select a hiding position that is out of view of the active shooter, provides a degree of ballistic protection, and permits freedom of movement.

e. Silence any electronic devices (e.g., cell phones) that may compromise the location.

f. Remain quiet.

g. If safe, allow others to take refuge in the location.

h. When first possible, notify security force members of the location and physical condition, number and types of casualties, and location of active shooter(s), if known.

i. If unable to communicate due to risk of compromise, leave the line open.

5. Taking action. When evacuation or finding a secure position are not options, or life is in imminent danger from the active shooter, the best course of action may be to disrupt and/or incapacitate the active shooter. The following considerations shall be taken into account:

a. When the active shooter is at close range and flight is impossible, the chance of survival is much greater if an individual tries to incapacitate the shooter.

b. Act as aggressively as possible.

c. Once committed to the actions, follow through.

d. Make use of available weapons and/or improvised weapons.

e. Distract the active shooter (e.g., throw items, yell).

f. Inform security force members when safe to do so.

g. Report critical information to security force members.

6. Security force response. While it is important to provide medical treatment to the wounded or injured, the primary duty of security force members responding is to protect innocent life by stopping the actions of an active shooter(s). Regardless of rank, the first security force member who is not part of the contact or rescue team to arrive on the scene of any active shooter shall become the incident commander and remains in that capacity until properly relieved. The incident commander shall do the following:

a. Establish an incident command post (ICP).

b. Determine response and staging area for arriving personnel.

c. Request additional resources (i.e., NSF response personnel, NCIS, local agency(ies)' special weapons and tactics team, or negotiator(s)).

d. Arrange a safe staging area for medical units and triage area.

e. If suspect is arrested or incapacitated, ensure the crime scene stays secure and maintains integrity until investigators or NCIS arrives.

1. Aircraft threat. The detect-to-engage sequence is when dealing with aircraft threats. Certain security aspects (e.g., determining temper, intent and weapons release authority) become more difficult. If aircraft are deemed to be hostile and security forces open fire with weapons, collateral damage from expended rounds is an added concern. While this risk also exists when firing on waterborne and land threats, the potential for collateral damage is greater when firing against an air threat.

2. Aircraft threat principles. Aircraft can be used as a weapon or to deliver another weapon (e.g., bomb, missile, or chemical/biological agent).

a. Visually assess aircraft near protected assets or areas.

c. Consider firing arcs and select weapons to minimize collateral damage. Responsible local air traffic control mechanisms (e.g., Federal Aviation Administration (FAA)) should warn suspected hostile aircraft of their position in relation to controlled air space and corridors. Noncompliance is not necessarily a hostile act, but if the aircraft continues on a collision course, the decision to engage must be made far enough in advance to be effective in stopping the potential attack. The ideal weapons for defense against aircraft threats are designated airborne assets and Crew Served Weapons. Although difficult to initially detect, small general aviation aircraft are relatively easy to destroy once hostile intent is established.

3. Aircraft threat procedures. The following procedures are used to deter an aircraft attack:

a. If credible intelligence anticipates a threat, consider the feasibility of making preparations for an attack.

b. Contact the RDC and request they request the FAA create a temporary restricted area.

c. Brief mobile patrols and sentries on the threat.

d. Ensure sentries have flares and spotlights to warn off suspicious aircraft.

e. Evaluate the feasibility of using ships' weapons systems (e.g., missiles/close-in weapons system).

f. Determine Crew Served Weapons and position them around the asset or area to be protected.

g. Coordinate security measures with local law enforcement agencies and Surface Combatants in the waterfront.

h. Ensure CBRNE gear and treatment measures are available.

1. **Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives.** Chemical, biological, radiological, nuclear and explosive defense (CBRNE) principles include contamination avoidance, protection, and decontamination. Contamination avoidance has a direct and significant impact on limiting the spread of contamination by isolating key resources from the need for decontamination. Early detection triggers the use of contamination avoidance procedures and protects personnel through the use of collective protection and IPE. The use of alarms and signals conveys early warnings of CBR contamination. Easily recognizable and reliable alarm methods enable units to respond quickly and correctly to CBR hazards. Standard alarms, nuclear, biological, and chemical (NBC) warning and reporting systems, and contamination markers help give orderly warning that may also require a change of mission-oriented protective posture (MOPP) level. Alarms and signals include:

a. Audible alarms.

b. Automatic alarms.

c. Visual signals.

Protection against the CBRNE threat can best be accomplished through the proactive application of passive defensive measures (those actions that a unit takes regardless of the CBRNE threat). Such practices enhance COOP through deterrence and defense. Passive protection measures include:

a. Realistic, integrated training.

b. Dispersing and employing camouflage, concealment, and deception.

c. Hardening of positions (ECPs, CSW positions).

d. Readying personnel (IPE, MOPP).

e. Remaining mobile.

f. Covering supplies and equipment.

Should decontamination be required as a result of a CBRNE attack the following principles guide through decontamination operations:

a. Speed, decontaminate as soon as possible to restore full combat potential.

b. Need, decontaminate only what is necessary. Consider mission, time, and extent of contamination, MOPP status, and decontamination assets available.

c. Limit, decontaminate as close to the site of contamination as possible to limit its spread.

d. Priority, decontaminate the most important items first and the least important items last.

2. Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Assault on an Entry Control Point. If threat elements attack the ECP with CBRNE devices, sentries should perform the following:

a. Engage the threat with lethal force if it is detected that they are executing the attack.

b. Immediately secure the ECP, and fall back into covered positions.

c. Don CBRNE PPE.

d. Activate alarms and signals.

e. Notify RDC with initial report of incident.

f. Control access to compromised areas.

g. Identify and isolate casualties.

h. Ashore equipment description:

(1) Chemical protective garments; Smock and Trousers.

(2) Protective Masks; M-40, M-45, MCU-2A/P.

(3) Medical Items; Atropine, 2-PAM Chloride, pyridostigmine bromide (PB), convulsant antidote for nerve agent (CANA).

i. Ashore MOPP Levels/Descriptions:

(1) MOPP 0/Carry Mask, IPE available.

(2) MOPP 1/Don over garment.

(3) MOPP 2/Don protective boots.

(4) MOPP 3/Don protective mask.

(5) MOPP 4/Don protective gloves.

j. Guide response forces (e.g., NSF teams, firefighters, HAZMAT response, and EOD).

k. Brief Incident Commander on status upon arrival. Concurrent with sentries actions, the CDO, and NSAW Watch Commander deploys reaction forces to mitigate effects of the attack and to prepare for a secondary attack.

3. Mailroom Attack. Terrorists have demonstrated the ability and motivation to send HAZMAT via letters or packages through postal systems. The damage incurred when these weapons achieve success depends on the agent or explosive employed.

4. Mailroom Attack Threat Principles. The following principles should be performed to counter a CBRNE mailroom threat:

a. Identify suspicious letters and packages.

b. Isolate suspicious letters and packages.

c. Notify Watch Commander.

d. Evacuate personnel.

e. Guide response forces (e.g., damage control teams, firefighters, HAZMAT response, and EOD).

f. In the event of exposure, execute the following actions:

(1) Immediately secure the mailroom, including ventilation systems.

(2) Evacuate all non-exposed personnel.

(3) Send initial incident voice report.

(4) Control access to exposed areas.

(5) Identify and isolate casualties.

(6) Guide response forces.

(7) Brief on-scene commander on status upon arrival.

5. Mailroom Attack Threat Procedures. The following procedures are used to counter a CBRNE mailroom threat:

a. Mailroom personnel are properly trained in the ID and isolation of suspicious letters and packages.

b. HAZMAT first responders are trained and equipped to respond to a threat.

c. Medical staffs are prepared to handle "dirty casualties" to include the activation of isolation areas and the conduct of proper triage.

d. Security personnel and first responders (e.g., emergency services and damage control teams) are outfitted with PPE.

e. At FPCON Charlie, or when credible intelligence indicates a valid threat, mail should be screened by a shore facility that has the capability to screen for CBRNE threats prior to arrival to its destination.

6. Simultaneous Attack. Various terrorist groups have the proven ability to launch simultaneous, coordinated attacks against multiple targets. Coordinated attacks indicate high levels of sophistication in planning, surveillance, target

selection, and mission execution. NSAW CO and ATO must be cognizant of this type of attack profile. These scenarios can include:

a. Land/land, land/sea, sea/sea, air/land and air/sea.

7. **Simultaneous Attack Procedures.** The following procedures are used to reduce exposure to simultaneous attacks:

a. Ensure security countermeasures are sufficient to defend against an attack, especially when personnel and assets are dispersed at various locations.

b. Maintain access to intelligence products that continually monitor terrorist operational profiles.

c. Implement RAMs to deceive the threat in regard to security force capabilities and dispositions.

d. Coordinate with Local Law Enforcement for security operations outside of the perimeter to interdict the attack prior to execution.

1. **Entry Control Point (ECP) threat.** The primary focus is the ability to detect and defend against attack by a terrorist/vehicle with an IED/VBIED. The approach is proactive in nature and emphasizes standardized procedures across all ashore ECPs should have clearly posted vehicle speed limit, traffic regulatory, and directional signs, and these directives should be strictly enforced. These signs must not impede the sentry's line of sight of oncoming traffic. Any person or vehicle that needs to reach a critical asset or area should be required to pass through an ECP. ECPs are typically base gates, pier accesses, and ships' quarterdecks. Such defense-in-depth is designed to keep pedestrian-carried IEDs and VBIEDs far enough from critical assets and areas (blast mitigation) to avoid serious damage.

2. **Personnel and vehicle identification.** The professional presentation of each sentry on watch is essential to deterrence. It is critical that all personnel and vehicles that approach an ECP are treated uniformly with judgment and discretion. Regardless of the fact that the sentry may know or recognize the individual or make of vehicle at the ECP, it should not be automatically assumed that the individual is cleared for entry without physically confirming proper ID. Terrorists have frequently used friendly uniforms, vehicles with familiar markings, and false ID to gain entry to unauthorized areas. Continual vigilance greatly enhances the security posture and contributes to both deterrence and detection. Before allowing personnel and vehicles to pass through an ECP, sentries shall perform the following procedures:

a. Check ID cards of all pedestrians and vehicle drivers. Check ID of vehicle passengers according to current policy.

b. Match picture on ID to bearer.

c. Ensure ID is authentic and has not expired.

d. Confiscate altered IDs, retain person, and turn over to a mobile patrol and notify the Watch Commander immediately.

e. Inspect personnel and hand-carried items according to current policy.

f. Ensure bearer is authorized entry according to current access policy or daily access list.

g. Detain unauthorized personnel attempting to gain access, request assistance from a mobile unit and notify the Watch Commander immediately.

h. Check vehicle ID papers.

i. Direct vehicles to inspection area and inspect according to current policy.

j. Deny access to unauthorized vehicles.

3. **Unauthorized pedestrian or vehicle.** Whenever possible, use the Final Denial Barriers to channel, slow, and physically stop the vehicle until it can be cleared to enter. The decision to authorize the UODF is influenced by the following considerations:

a. Justifications for deadly force as detailed in the rules for the UODF.

b. Conspicuousness of the warning to stop.

c. Potential targets protected by the ECP, to include sensitivity, classification, and operational importance of the area, as well as the nature of the potential targets inside (e.g., VIPs and large occupancy buildings).

d. Latest threat warning and current FPCON levels.

e. The number of and means by which the suspect negotiated the obstacles or barriers protecting the ECP.

f. Any indications that the vehicle poses a specific threat capability (e.g., visible explosives or symbols, visible weapons, type of vehicle, and HAZMAT symbols).

g. Indications of intent (e.g., evident duress or nervousness of the suspect(s), threatening statements, and clothing (hoods, masks, body armor, and explosive vests)). Unless operating under the ROE/RUF that state otherwise, no sentry engages a driver or vehicle with weapons fire unless conditions of extreme necessity exist and the UODF is justifiable as described in SECNAVINST 5500.29 (series), Use of Deadly Force and the Carrying of Firearms by Personnel of the Department of the Navy in Conjunction with Law Enforcement, Security Duties, and Personal Protection. When the decision is made to use deadly force, the ECP sentry should direct fire at the tires, engine, windshield, and driver. When the PPR does not authorize deadly force, perform the following procedures:

(1) Stop the vehicle using the Final Denial Barriers.

(2) Notify RDC of the threat (to include description and direction of travel).

(3) Attempt to identify the nature of the threat (capability, opportunity, and intent).

(4) Take the necessary action to neutralize the threat to include:

(a) Inform the innocent, unaware, or mentally diminished.

(b) Detain those who are suspicious, but otherwise non-threatening (using standard procedures for a traffic stop).

(c) Apprehend the inebriated or those suspected of other offenses not involving a hostile threat.

(d) Contain those who present a continuing threat upon analysis of capability, opportunity, and intent.

h. After taking immediate action, secure the ECP until the incident is resolved.

4. Protests and rallies. If protestors approach an ECP, the sentry should perform the following procedures:

a. Upon initial gathering or massing of personnel, notify RDC and the Watch Commander.

b. Prepare to secure ECP by closing gates or activating Final Denial Barriers.

c. Maintain the flow of friendly personnel through the ECP.

d. Do not take actions that would escalate the situation.

e. Request reinforcements (additional mobile units).

f. Verbally warn protestors to remain away from the post as directed by the Watch Commander.

g. If protestors physically attack sentries or attempt to forcefully gain access to the protected area, sentries will perform the following procedures:

(1) Prevent access by using authorized force.

(2) Apprehend aggressors and remove from immediate area.

(3) Secure ECP as directed to prevent unauthorized access.

(4) Assist civilian authorities as required.

(5) Maintain positive access control at all times.

h. Photograph participants (which can be an effective deterrent, and it removes anonymity from the process).

5. Media requests. Representatives of the media are not allowed access to the protected area without proper authorization. Sentries should proceed as follows:

a. Notify Watch Commander when media representatives do not identify themselves, attempt to gain access to the protected

area, or are visibly present near the ECP displaying cameras, lighting, sound equipment, or marked vehicles.

a. Refer all media queries to the proper military authority (e.g., the public affairs officer/command spokesperson, CDO, executive officer, or CO).

6. **Pedestrian-carried improvised explosive device.** When a pedestrian-carried IED is discovered, it should be treated as an attack with a deadly weapon, and deadly force is immediately authorized. While a weapon may be useful for an IED situation, the best survival tools are cover, distance from the IED, and time to achieve both. The ECP is the first line of defense against an enemy attack and the most likely to take casualties. It is the duty of each sentry to ensure they stop the aggressors at the ECP and prevent/deny access to the Installation.

NOTERadios should not be used around explosive devices as the radio waves may inadvertently detonate the explosives. A pedestrian-carried IED can be delivered by two methods:

a. Wearing the IED

b. Carrying the IED in a bag or case. Upon discovering an IED, the sentry should immediately communicate the presence of the IED to the cover team while simultaneously drawing his weapon. Cover team personnel should react to the contact sentry's actions by taking cover for protection from the blast and for good firing positions to engage the suspect(s) and provide the contact sentry fire support. While the cover team is providing fire support for the contact sentry, it should also initiate the loss of communications plan to the chief of the guard to indicate the ECP is under attack.

7. **Pedestrian-carried improvised explosive device on the suspect.** The most hazardous delivery method for security forces is to have an IED attached to the body of a suspect, like a piece of clothing (e.g., vest). This method is commonly employed by suicide bombers.

8. Contact sentry. The contact sentry should take the following actions:

a. Immediately communicate the presence of the suspected person to the cover sentry present at the location while simultaneously drawing weapon.

b. Begin giving verbal commands for the suspect to move to a position allowing for standoff distance from the sentry and any bystanders. Order the suspect to lie face down on the ground. Security personnel should not close in with a suspect wearing a visible IED.

c. While giving these commands, notify surrounding personnel to vacate the area immediately for their safety or, at a minimum, to stand clear at a specified distance.

d. If at any time during these actions the suspect makes a furtive motion indicating he is about to detonate the device, the contact/cover sentry should attempt a head shot between the suspect's eyes. A center mass shot may not penetrate enough to kill the suspect and may sympathetically detonate the explosives.

e. If a safe perimeter has been established around the suspect, seek cover at a safe distance but within accurate shooting range from the suspect.

f. From this position, command the suspect to remove the explosive device, and then provide instructions to proceed slowly to a location where the suspect can be safely apprehended.

g. If the explosive device is removed from the suspect, at least one sentry is designated to watch over the explosive device; he remains as such until relieved or until EOD arrives and disposes of the device.

h. Use deadly force if at any time the suspect disregards directions and attempts to make access to the perimeter, closes the gap between the contact sentry, or attempts to flee.

9. Cover team. For a suspect wearing an IED, the cover team should follow the actions listed below:

a. The cover team should take up firing positions, if not there already, that provide the best fire support for the contact sentry and protection from an impending explosion. Provide cover fire and support of any kind to protect the contact sentry and to ensure the security perimeter is not breached.

b. If there is more than one member of the cover team, the other individuals should secure the ECP (if not already accomplished by the contact sentry) by closing gates, activating the Final Denial Barriers and assist in getting non-combatants to vacate the area in order to establish a safe perimeter around the suspect. The cover team must not allow an explosion to incapacitate all members, leaving the ECP unguarded.

c. The cover team should initiate the loss of communications plan (send a messenger) and contact the Watch Commander. The team must not use radio communications, as radio waves could detonate the explosive device.

d. Once reaction forces have arrived, the cover team should take up defensive positions in the event that the IED is detonated and serves as the precursor for a follow-on assault.

e. Once a line of defense is established to protect against an initial and follow-on assault, the cover sentry can assist the contact sentry in controlling the suspect (if separated from the IED) while other members of the cover team and reaction force establish a safe perimeter around the suspect (if still attached to the IED) or the IED (if the two have been separated).

f. The team shall maintain the perimeter until EOD can arrive and dispose of the explosive device.

g. The team shall use deadly force if at any time the suspect disregards directions and attempts to make access to the perimeter, closes the gap between the contact sentry, or attempts to flee while still wearing the IED.

10. Pedestrian-carried improvised explosive device in suspect baggage. The other delivery method for a pedestrian-carried IED is carrying it in a bag or case so it can be left at a specific location, allowing the suspect to clear the area before it explodes. If an IED is discovered at an ECP inside a searched bag, sentries should take the following actions:

a. Communicate presence of suspect item to the cover team present at the location.

b. Initiate the loss of communications plan (send a messenger) to the Watch Commander (a radio signal could detonate the explosive).

c. Verbally command the suspect to move away from the suspected item. If the suspect is uncooperative, take physical control of the suspect and move away from the suspected item.

d. Once safely away or behind cover from the IED, restrain and search suspect.

e. Secure ECP by closing gates and activating barriers.

f. Direct all unarmed personnel to stand clear at specified distance.

g. Fall back and wait for EOD.

11. Unattended package at or near the entry control point. When an unattended package is noticed at or near the ECP, sentries should perform the following procedures:

a. Communicate the presence of the suspect item to the cover team.

b. Initiate loss of communications plan (send a messenger) to the Watch Commander. Secure use of cell phones as well as hand-held radios.

c. Secure ECP by closing gates and/or activating Final Denial Barriers.

d. Direct all personnel to stand clear of suspected IEDs or explosive material at a specified distance.

e. Remain alert for a secondary event or attack.

f. Maintain the integrity of the perimeter at all times.

12. Vehicle-borne improvised explosive device. A VBIED can be much more lethal than a pedestrian-carried IED due to the greater payload a vehicle is capable of delivering. A VBIED must be dealt with decisively to prevent it from accessing greater numbers of personnel and assets inside the perimeter being guarded. A VBIED could be targeting the ECP or attempting to access a protected asset, or it could also be the precursor to a follow-on attack. ECP personnel must carefully consider and rehearse PPRs to ensure effective and decisive action in stopping the threat outside the protected perimeter.

a. Contact Sentry, Upon determining or suspecting the presence of a VBIED, the contact sentry should take the following actions:

(1) Immediately communicate the presence of the suspected device to the cover team present while simultaneously drawing weapon and giving verbal commands for the driver and passengers to exit the vehicle, keeping their hands in sight.

(2) Direct driver and passengers to lie face-down with their hands behind their backs until they have been secured.

(3) Once they are secured, take suspects to a safe area, and hold while EOD is contacted.

(4) If the driver makes a furtive motion to run the gate, engage the driver with deadly force.

b. Cover Team should take the following actions:

(1) Activate Final Denial Barriers/close gate to stop the flow of traffic through the ECP.

(2) Take cover which affords good firing positions to engage the suspect vehicle and provide the contact sentry cover.

(3) Initiate the loss of communications plan (send a messenger) to the Watch Commander (a radio signal could detonate the explosive).

(4) Maintain cover when reaction forces arrive and take up defensive positions in the event that the VBIED is detonated and serves as the precursor for a follow-on assault.

(5) Once a line of defense is established to protect against an initial and follow-on assault, work with reaction force to establish a safe perimeter around the VBIED while the cover sentry assists the contact sentry in controlling suspects.

(6) Maintain the perimeter until EOD can arrive and dispose of the explosive device.

13. **Surveillance detection.** When there is suspicion or detection that the ECP or other asset is being observed, sentries should perform the following procedures:

a. Note suspect's physical characteristics, vehicle (if present), method of surveillance (e.g., cameras, video, and binoculars), and exact location.

b. Notify the chief of the guard/patrol supervisor or ECP supervisor using means other than a radio to avoid alerting observers who might be monitoring radio frequencies.

c. Maintain visual contact, and report any changes in location or suspect descriptions until the arrival of responding personnel.

14. **Medical emergency.** If there is a medical emergency at or near the ECP, sentries perform the following procedures:

a. Communicate situation to the Watch Commander.

b. Determine whether or not the victim requires first aid or emergency medical personnel.

NOTEDetermine if there is a legitimate medical emergency and not a pretense for terrorists to drive an ambulance onto an installation. Positively identify the emergency responders.

c. Maintain positive control of the ECP at all times. Secure ECPs only if necessary to provide first aid to the victim.

d. Direct responders to the victim.

1. Man-portable air defense system threat. Potential damage and loss of life resulting from the employment of MANPADS is greater than from a sniper or mortar threat. The November 2002 terrorist attack on an Israeli airliner in Kenya highlights the potential anti-air MANPADS threat to assets. Since MANPADS threats typically launch a single missile (fire and flee) as opposed to a recurring sniper or mortar threat, the key to countering the threat is to prevent its recurrence. The following criteria identify possible terrorist MANPADS launch sites:

a. Accessibility and concealment. A desirable location is one chosen for ease of ingress/egress and one that is concealed enough to allow the hostile fire team to get into position, assemble the weapon, and fire it without being discovered by security force personnel.

b. Line of sight, the terrorist needs an unobstructed view of the target.

c. Exposure time, this refers to the amount of time the intended target is vulnerable from an operational attack.

d. Distance to target, this is the distance required by a terrorist to positively identify the intended target.

2. Man-portable air defense system threat principles. The following principles apply to countering a MANPADS threat:

a. Lessen the number of potential targets on the ground by reducing the visibility of critical assets.

b. Extend sentries focus beyond the area immediately around the asset in order to assess potential MANPADS threats.

c. Increase presence of security forces beyond the perimeter to include mobile and foot patrols.

3. Man-portable air defense system threat procedures. The following measures should be employed to counter the MANPADS threat at airfields/installations and to reduce aircraft in-flight susceptibility. The following procedures are used to counter a MANPADS threat:

a. Identify areas of vulnerability in terms of possible launch sites, to include arrival and departure corridors and potentially vulnerable ground targets (e.g., Ships in the harbor or areas of mass gathering).

b. Obtain latest intelligence about MANPADS threat from the Air Mobility Command (AMC) worldwide database.

d. Analyze risks, and alter, divert, or cancel missions if the MANPADS threat is too great to mitigate.

4. Installation Defense Procedures. The following procedures are used for installation defense and to counter a MANPADS threat:

a. Isolate prime MANPADS launch sites and vulnerable areas by expanding the installations area of control. The following measures require coordination with local law enforcement.

(1) Increased physical presence at prime launch sites.

(2) Focused and random patrols of vulnerable areas.

(3) Electronic surveillance of vulnerable areas to include launch sites and potential targets.

b. Ensure personnel understand the MANPADS threat (to include component recognition), areas of vulnerability, and reaction plans.

c. Enforce installation access control procedures.

d. Disperse areas of mass gathering to reduce damage from a MANPADS or RPG attack.

1. Railborne improvised explosive device threat. Railborne IEDs have not been used to inflict terrorist damage, although the potential exists. The train's size permits loading very large IEDs with less likelihood of early discovery. The following are reasons a railborne IED is an attractive form of attack for terrorists:

a. The IED is easily transportable.

b. The size of the IED can be large and is not limited to what a person can carry.

c. A rail car is an inconspicuous delivery vehicle.

d. An IED can be easily hidden within a rail car.

2. Railborne Improvised Explosive Device Threat Principles. The following principles provide guidance to counter railborne IEDs:

a. Prevent the IED from reaching a critical asset or area.

b. Minimize loss of life and property should an incident occur.

c. Limit the number of ECPs.

3. Railborne improvised explosive device threat procedures. The following procedures are used for responding to a railborne IED threat:

a. Report the incident to RDC and request assistance from local law enforcement and Federal Fire department.

b. Establish and maintain perimeter of affected area.

c. Establish an Incident Command Post and Incident Commander.

d. Maintain surveillance or control of the scene until the threat no longer exist.

1. Small boat threat. On 12 October 2000, the USS COLE, assigned to the US Fifth Fleet, was the target of a small boat attack in the Port of Aden, Yemen. Approximately two hours after the ship moored in the harbor for refueling, a two-manned fifteen-foot skiff packed with several hundred pounds of C-4 military explosives circled her bow before closing amidships and detonating the charge. Threats to HVAs must be considered and do exist.

2. Deep draft threat. Deep draft ships have the potential to inflict devastating damage due to their large capacity to hold explosives and to the difficulty friendly forces face trying to stop an underway vessel. Security forces and boats can stop hostile small vessels by shouldering, ramming, or shooting them. Although the same measures could be employed against an approaching hostile ship, the likelihood of stopping it is minimal.

3. Deep draft threat procedures. Procedures to counter a deep draft threat follow:

a. Coordinate with Port Operations and Coast Guard assets for daily vessel movement schedule for Naval Support Activity Washington AOR.

b. Coordinate with USCG for vessel boarding and the emplacement of USCG assets.

c. Coordinate with local law enforcement, Coast Guard Units to identify pre-staging/standoff area for high-interest vessels

4. Subsurface threat. The waterborne threat occurs at the subsurface level, carried out by swimmers/divers or mines, or a combination of the two. Subsurface threats are an attractive option for terrorists because of their relatively low cost and simplicity. The most difficult aspect when planning to defend against subsurface threats is employment of capability to detect and identify hostile intent. Security forces may not see a swimmer/diver or mine until it is in the reaction zone. While a mine is clearly a threat and should be acted upon immediately, a swimmer/diver or bubbles in the water are not necessarily indicative of a hostile threat, and deadly force may not be the correct response.

5. Subsurface threat principles. The following principles guide in the detection and deterrence of subsurface threats:

a. For reacting to a surfaced swimmer/diver or bubbles sighting. The following questions ensure that security forces are armed with sufficient authority to counter this elusive threat:

(1) Is any swimmer/diver in the water within a certain distance from the protected asset or area assumed to be hostile?

(2) Can concussion grenades automatically be used if a swimmer/diver submerges or bubbles are seen?

6. Subsurface threat procedures. PPRs to defend against swimmer/diver and floating mine threats are primarily the same, though some differences do exist. The following procedures are used to counter a subsurface threat:

a. Analyze general layout of harbor/anchorage to include:

(1) ID of possible launch points for swimmers, divers, and floating mines (e.g., marinas, storm drains, and piers)

b. Adhere to waterside security perimeter and assessment, warning, and threat zones.

c. Utilize local support (e.g., security boats, landward security, marine mammals, fixed sensors, EOD, fire, medical, and communications).

7. Swimmer/diver procedures. Additional procedures to counter a swimmer/diver follow:

a. Define waterside security perimeter and assessment, warning, and threat zones based on the approximate axis of approach.

b. Analyze pier construction and layout.

c. Analyze general layout of harbor/anchorage to identify possible swimmer/diver cover areas.

d. Construct and deploy warning bells (e.g., multiple treble hooks, chemical lights, and bells on 15-foot light fishing line at random intervals along the waterline) which are

effective against swimmers/divers but may be difficult to maintain and redeploy.

e. Determine weapons and measures to be used against swimmers/divers including:

(1) Security boat weapons (CSWs)

(2) Concussion grenades

(3) Diver recall devices

(4) Mobile units positioned along the waterside perimeter.

f. Identify floating debris that could be used as camouflage.

g. Randomly conduct Riverwalk patrols. Lookouts should be alert for signs of swimmers/divers (e.g., air bubbles, snorkels, and piles of floating debris used to conceal a swimmer).

8. Anti-swimmer continuum of force. Effective procedures to counter a swimmer attack follow:

a. Warn swimmer using any means available that swimmer/diver is in a restricted area and will be fired on if swimmer does not remain on/return to surface.

9. Mine/underwater improvised explosive device procedures. Mines/UWIEDs can either be attached to a ship's hull/pier structure, or floated in the water and drifted toward a ship/pier. Tactical considerations to counter these methods differ as outlined below.

10. Limpet mines/underwater improvised explosive devices. The following procedures are used to counter a limpet mine/UWIED:

a. Adhere to anti-swimmer procedures

b. In the presence of a specific mine threat, or if a mine is spotted, take the following actions:

(1) Notify EOD, Coast Guard Units, and local law enforcement.

(2) Deploy supporting agencies from the most practical location to conduct mine neutralization. Prior to conducting a hull search following a suspected swimmer/diver or other potential mine event, institute an emergency dive bill (if available)

11. Countering floating mines/underwater improvised explosive devices. The following procedures counter floating mines/UWIEDs:

a. If the threat of mines exists, follow the additional preplanned measures:

(1) Establish security perimeter with booms to block mines, if available.

(2) Post lookouts on the piers, coordinate with afloat units to use topside rovers, brief with visual profiles of threat mines/UWIEDs, if any.

b. In the presence of a specific mine threat, or if a mine is spotted, follow the actions below:

(1) Notify the DS Barry so they can set material condition Zebra.

(2) Notify EOD and local law enforcement authorities.

c. Deploy supporting agencies from best practical location to conduct mine neutralization.

1. **Standoff attack threat.** As demonstrated by the attack on the amphibious assault ship (dock) USS KEARSARGE (LHD 3) and the landing ship dock USS ASHLAND (LSD 48) while pier-side in Aqaba, Jordan, one of the most difficult threats to detect, deter, and defend against is a standoff attack because close contact is never made between the attacker and security forces. The most likely standoff threats are snipers, mortars, RPGs, and MANPADS (e.g., Stinger missile); Snipers use rifles as antipersonnel weapons, while mortars and RPGs are primarily anti-equipment weapons.

2. **Standoff Attack Threat Principles.** The best way to defeat a standoff threat is prevention. The following principles serve as a guide to counter a standoff threat:

a. Lessen the number of potential targets by reducing the visibility of critical assets and areas.

b. Extend sentries focus beyond the area immediately around the asset in order to assess potential standoff threats.

c. Maintain the capability to communicate with local law enforcement authorities to quickly counter standoff threats.

3. **Standoff Attack Threat Procedures.** The following procedures are used to counter a standoff attack:

a. Determine sniper, mortar, and RPG areas that are most likely to support an attack with standoff weapons.

b. Minimize the number of personnel topside.

c. Reduce ID lighting.

d. Harden sentry posts.

e. Provide sentry with binoculars and NVGs(available).

f. Is practical, coordinate with Port Operations to use pier equipment (e.g., cranes and containers) to disrupt the line of fire from the most likely threat sector.

g. Do not draw attention to the arrival or presence of VIPs (e.g., the use of pennants on ships).

h. Communicate and coordinate with local law enforcement to patrol the most likely danger areas.

1. **Surveillance.** Before initiating an attack, terrorists conduct months or years of meticulous planning to maximize the likelihood of success. Terrorists gather exhaustive operational knowledge of a target through surveillance. They examine all details of a target, including watch schedules, ECP procedures, periodicity of roving patrols, volume of traffic, citizenship of security guards, and the presence of defensive weapons. Navy assets and areas are actively being considered as targets of opportunity.

2. **Surveillance detection principles.** Surveillance detection is conducted to record the activities of persons behaving in a suspicious manner and to report such information in a format that is usable by the appropriate command, LE or intelligence officials. The following principles serve as a guide to detect suspicious surveillance activities:

a. All personnel are potential observers of surveillance activities.

b. All personnel must have a heightened awareness of their surroundings.

c. Intelligence about potential local terrorist activity must be disseminated to all personnel.

d. Suspicious activity must be reported up the chain of command and to security forces.

3. **Surveillance detection planning procedures.** Surveillance methods include both mobile and fixed personnel and devices. Mobile surveillance means following targets to discern their patterns and routines. Multiple terrorist operatives can be employed to trail targets as they move from place to place. In fixed surveillance, terrorist personnel and devices stay in one spot to observe the target. A discrete observation point can be established in a house, office, commercial business, or parked vehicle. Using fixed and static surveillance, terrorists can observe buildings, facilities, ships, and bases. Terrorists use various modes of transportation (e.g., buses, trains, or boats) to approach and observe entry control procedures and the reaction of security forces.

4. Detecting surveillance activity. Successful surveillance detection requires knowing what to look for and being able to distinguish the ordinary from the extraordinary. Surveillance detection is watching for persons observing personnel, ships, and installations. Personnel, especially sentries, must become familiar with their surroundings and normal installation operating procedures. Heightened awareness, personnel must be able to detect the slightest changes, which may be indicators of surveillance activity. Terrorist surveillance detection activities include the following:

a. Multiple sightings of the same suspicious person, vehicle, or activity, separated by time, distance, or direction.

b. Individuals staying at bus stops for extended periods while buses arrive and depart.

c. Individuals engaging in long conversations on cellular telephone.

d. Individuals ordering food at a restaurant and leaving before the food arrives or ordering without eating.

e. Joggers standing and stretching for an inordinate amount of time.

f. Individuals sitting in a parked car for an extended period of time.

g. Individuals wearing improper attire for the location (or season) and not fitting into the surrounding environment.

h. Individuals drawing pictures/taking notes or photographs in an area not normally of interest to a standard tourist; showing interest in security cameras and sentry locations; or noticeably watching security reaction drills and procedures.

i. Individuals exhibiting unusual behavior (e.g., staring at or quickly looking away from individuals or vehicles as they enter or leave designated facilities or parking areas).

j. False phone threats.

k. Individuals approaching security checkpoints to ask for directions or "innocently" attempting to smuggle nonlethal contraband through checkpoints in order to determine the effectiveness of search procedures and to gauge the alertness and reaction of security personnel.

l. Vehicle breakdowns on or near installations or ECPs.

m. Vehicles with an excessive number of antennas (possibly indicating two-way radios).

n. Personnel or vehicles performing evasive movements.

o. A dirty vehicle with a clean license plate or vice versa, indicating a recent change.

5. **Reporting surveillance activity.** Personnel detecting or suspecting surveillance of assets or areas should immediately report it to the chain of command. Sentries should have the ability to note descriptions and details of any suspected surveillance activity. All reporting should be in compliance with OPNAVINST 3100.6 (series).

NOTEUntrained personnel should avoid confrontation with suspicious individuals. Surveillance detection techniques must be specific in order to be effective. Observers must note the following information:

a. Detailed descriptions of suspicious personnel to include:

(1) Gender, height, weight, hair color, build, race, and identifying marks.

(2) Clothing.

(3) Equipment carried by suspicious personnel (e.g., a phone, camera, or notebook).

b. Time of day.

c. Exact location of suspicious activity.

d. Detailed description of vehicle.

6. **Surveillance detection countermeasures.** Surveillance detection countermeasures to deter terrorist activities include installing mechanical devices, varying modes of watch stander behavior, and employing physical barriers. Effective countermeasures specifically include the following:

a. Displaying visible security cameras and motion sensors.

b. Employing random AT measures to include:

(1) Roving security patrols with varying size, timing, and routes.

(2) Sentry watch rotations.

(3) Active searches (including x-ray machines and explosive detection devices) of vehicles and personnel at ECPs.

(4) EDD teams at ECPs.

c. Emplacing barriers, roadblocks, and entry mazes.

d. Visibly displaying CSW and sentries.

e. Properly equipping sentries with NVGs, binoculars, thermal imagers, and other gear to enhance surveillance detection.

f. Ensuring sentries receive training in detecting surveillance activities.

g. Establishing sentry posts to ensure all potential surveillance locations can be observed.

h. Ensuring a camera is readily available for surveillance detection. Surveillance detection measures assist personnel with consistently maintaining a vigilant stance. By proactively watching for suspicious activity, observers have the highest chance of deterring terrorist attacks before they become a reality.

7. **Surveillance Detection Training.** Surveillance detection units are trained by NCIS STAATs. Training objectives include terrorist methodology and facility, area, and route analysis.

Training culminates with a final exercise and a written test. In addition, DHS provides surveillance detection training for commercial infrastructure operators and security staff.