



LEVEL I ANTITERRORISM (AT) AWARENESS TRAINING FOR IMT/BOLC





TERMINAL LEARNING OBJECTIVE

- **Action:** Develop Antiterrorism Awareness in DoD Personnel.
- **Condition:** In a garrison environment, given a lesson plan, presentation, handouts, reference materials and a regulatory requirement to conduct Antiterrorism Awareness Training.
- **Standard:** Develop antiterrorism awareness in DoD personnel so they can identify threats and implement individual protective measures. Identify the five Force Protection Conditions, three responses for an active shooter and two indicators of enemy surveillance without error.



ADMINISTRATIVE INFORMATION

- **Safety Requirements:** No major considerations
- **Risk Assessment Level:** Low
- **Environmental Consideration:** No major considerations
- **Evaluation:** Checks on Learning



TODAY'S THREATS (VIDEO)





TERRORIST TACTICS AND OPS

- Terrorist tactics and operations consistently change to exploit our vulnerabilities. Common tactics used by terrorists are as follows:
 - Bombings (IEDs, VBIED, Suicide Bombings, Mail)
 - Shootings (Active Shooter, Snipers, Ambushes)
 - Edged Weapon Attacks (Knife, Machete, Axe)
 - CBRN Attacks (Ricin, Anthrax, etc.)
- Obtain threat information from your S-2.
- Use Individual Protective Measures to protect against threats.



DOD THREAT LEVELS

- Intelligence staff officers develop threat assessments used to determine threat levels for the AOR.
- Low - No group is detected or the group activity is non-threatening.
- Moderate - Terrorists are present but there are no indications of anti-U.S. activity. The operating environment favors the HN/U.S.
- Significant - Anti-U.S. terrorists are present and attack personnel as their preferred method of operation or a group uses large casualty producing attacks as their preferred method but has limited operational activity. The operating environment is neutral.
- High - Terrorists are operationally active and use large casualty producing attacks as their preferred method of operation. The operating environment favors the terrorist.



FPCON MEASURES

The DOD FPCON system has progressive levels of protective security measures implemented in response to terrorist threats.

Normal – Always applies because of the general threat of terrorism around the world.

Alpha - Applies to a non-specific threats directed against DOD elements and personnel.



FPCON MEASURES CONT.

Bravo - Applies when an increased or more predictable threats exists and are directed against DOD elements and personnel.

Charlie - Applies when an attack occurs within the commander's (AOI), or intelligence is received indicating an attack is likely.

Delta - Applies when an terrorist attack occurs or is anticipated against specific installations or operating areas.



CHECK ON LEARNING

- How many Force Protection Measures are there in the DoD FPCON system?

Five

- What FPCON measure provides the most protection?

FPCON Delta



INDIVIDUAL PROTECTIVE MEASURES (IPM)

- CJCS 5260 provides information on IPM.
 - Guard information about yourself and your job.
 - Limit signs of your DOD affiliation off base.
 - Limit access to personal information.
 - Practice OPSEC.
 - Avoid established or predictable patterns.
- Recognize and Report Suspicious Activity.
 - Report to your chain of command, MI (1-800-Call-Spy), MPs, local police, or FBI.



INSIDER THREAT INDICATORS

- Anti-American statements.
- Aggression or threats towards coworkers.
- Presence of unauthorized weapons.
- Association with extremist groups.
- Distribution of extremist propaganda materials
- Allegations of US persecution against a group or religion.
- Repeated violation of policies.
- Abuse of alcohol or drugs.



MAKING TRAVEL ARRANGEMENTS

- OCONUS Travel:
 - Get an AOR threat briefing prior to travel.
 - Consult the DoD Foreign Clearance Guide.
 - Reserve government quarters or contracted hotels.
 - Ensure that your Level I Awareness training is current.
 - Know the location of the U.S. Embassy.



TRANSIT SECURITY

- Americans may be vulnerable to attack or kidnapping while in transit. This is especially important when overseas.
- Perform the following security measures when in transit:

Vehicle Security Measures:

- Look for tampering around, under, and in your car.
- Keep doors locked and windows rolled up.
- Vary routes, travel times, and parking places.



TRANSIT SECURITY CONT.

- Public Transportation Security Measures:
 - Vary travel times, routes, and taxi companies.
 - Match taxi drivers' faces to taxi licenses.
 - Avoid crowded places on subway and train platforms and at bus stops.
 - Secure doors on train sleeper cars.



TRANSIT SECURITY CONT.

Air Transit Security Measures:

- Do not fly routes with stops in high risk areas.
- Proceed to the secure areas as soon as possible.
- Report suspicious/unusual activity.
- Do Not Fly in Uniform.
- Wear Conservative Civilian Clothing.





AIR TRANSIT SECURITY MEASURES CONT.

- Seat Selection:
 - Sit near an emergency exit or as close as possible.
 - Window seats offer protection.
 - Aisle seats offer options.
- If hijacked:
 - Remain calm.
 - Hide all military related documents.
 - Identify hijacker(s)' intentions.
 - Use your best judgement if and when to take action.





HOTEL SECURITY MEASURES

- Hotel security measures to consider:
 - Perimeter security.
 - Sufficient standoff distance from the street.
 - Access Control
 - Avoid rooms on the 1st and 2nd floors.
 - Avoid rooms above the 7th floor.
 - Leave the lights and TV on when leaving the room.
 - Keep the curtains closed.



RESIDENTIAL SECURITY MEASURES

- Use residential security measures to protect your home and family:
 - Brief the family on the residential security/safety plan.
 - Have a duress word for the family.
 - Have sufficient lighting, locks, to meet the local threat.
 - Keep the house locked.
 - Do not leave keys hidden on the property.
 - Maintain friendly relations with your neighbors.
 - Keep yourself informed of potential threats.



SUSPICIOUS PACKAGES

- Beware of suspicious packages that have any of the following:
 - Unusual odors.
 - Protruding wires or strings.
 - Oily stains on the package.
 - Excessive postage.
 - No return address or unfamiliar return address.
 - Incorrect spelling or poor typing.
- Clear the area immediately and notify your chain of command and local authorities.



CHECK ON LEARNING

- How should you dress when traveling?

Wear conservative civilian clothing and do not carry military style bags.

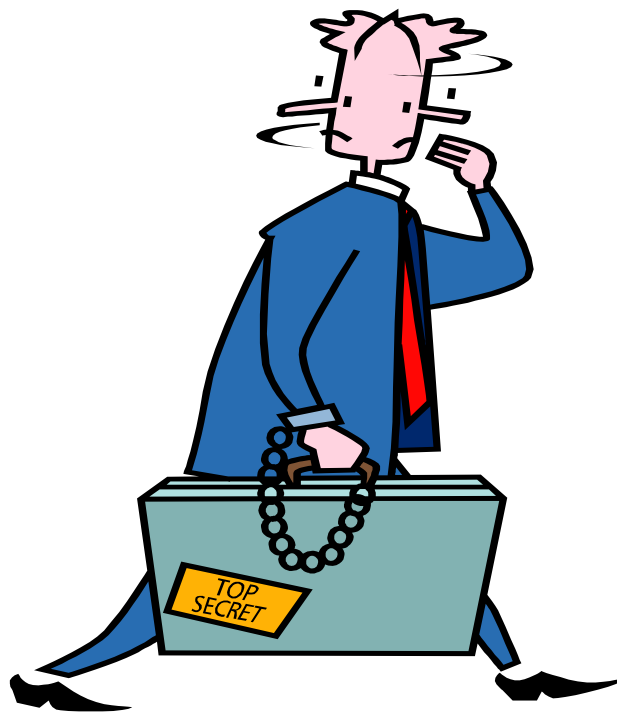
- Where is the safest part of the airport?

Past the security screening area



DETECTING SURVEILLANCE

- Some type of surveillance precedes every terrorist attack.
- Early detection of terrorist surveillance is often a matter of life or death.





SURVEILLANCE

The Secretive, Continuous and Sometimes Periodic
Watching of Persons, Vehicles, Places or Objects to
Obtain

INFORMATION





TERRORIST SURVEILLANCE TECHNIQUES

- Terrorists may use continuous fixed, mobile or progressive surveillance techniques of a specific target.
- Be aware of the following indicators:
- Multiple sightings of the same suspicious person, vehicle, or activity separated by time, distance, or location.
- Individuals who stay at bus stops for extended periods of time when the buses come and go.
- Individuals who order food at restaurants and then leave before the food arrives or order without eating.



INDICATORS OF SURVEILLANCE

- Individuals drawing pictures or taking notes in an area not normally of interest to a tourist
- Photographing security cameras, guard locations
- Jogger who stand and stretch for an inordinate amount of time
- Individuals who don't fit the surrounding environment



PASSIVE MANEUVERS

- Passive maneuvers are techniques to identify mobile surveillance.
 - Check your mirror during turns to confirm surveillance.
 - If walking, check the reflection in the windows of buildings to determine if you are being followed.
 - Travel around the block.
 - Do not drive home.
 - Note the description of the vehicle or person following you.
 - Go to the nearest military base or police station.
 - Report the incident to law enforcement.





TERRORIST USE OF SOCIAL MEDIA

- Terrorists use social media as a method of surveillance, recruitment and to spread propaganda.
 - Al Qaeda posted a handbook on social media informing their followers to conduct surveillance on service members and their families.
 - This information is used to plan and conduct attacks.
 - Terrorists conduct phishing schemes to load malicious code.
- Don't share your job title, work or family information, or hobbies.
- Don't share any Personally Identifiable Information (PII).



PERSONALLY IDENTIFIABLE INFORMATION (PII)

- Personally Identifiable Information (PII) is any information that someone can use to distinguish or trace an individual's identity.
- Criminals or terrorist can obtain PII through the following:
 - Social media
 - Network intrusions
 - Stealing laptop computers
 - Not shredding documents containing PII



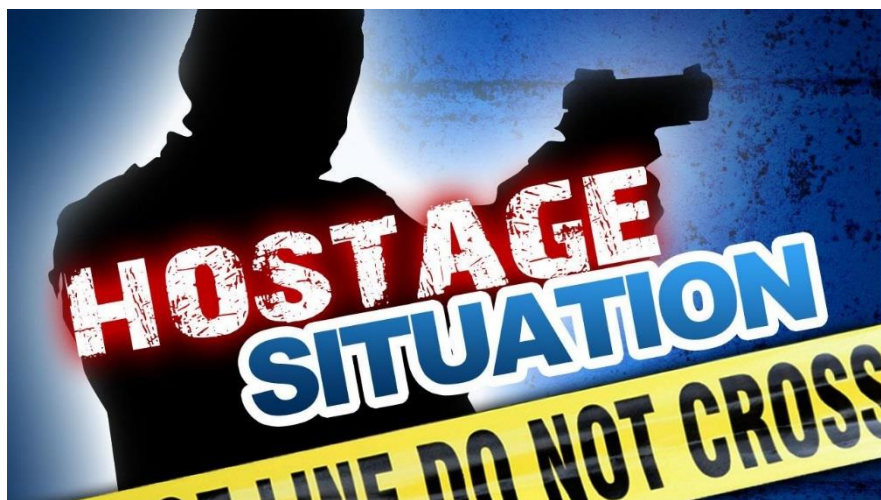
CHECK ON LEARNING

- What are some indicators of surveillance?
 - Multiple sightings of the same person, vehicle, or activity.
 - Individuals at bus stops that are still there when the bus leaves.
 - Individuals who order food at restaurants and then leave before the food arrives or order without eating.
 - Photographing security cameras, guard locations.
 - Jogger who stand and stretch for an inordinate amount of time.
 - Individuals who don't fit the surrounding environment



HOSTAGE SURVIVAL

A tool used by terrorists, foreign governments and criminals to gain control over a situation.





BARGAINING CHIPS

- Hostages are valuable to foreign governments, criminals, or terrorist organizations; however, if a hostage becomes a liability, he/she may be killed.





TO IMPROVE SURVIVAL ODDS

- Have situational awareness
- Remain calm

If escape is not possible:

- Display a non-threatening (but not submissive) posture
- Follow instructions
- Avoid sudden movements



HOSTAGE STRATEGIES

Establish rapport:

- Introduce commonalities
- Active Listening
- Address captors by name (if known)
- Avoid emotionally charged topics (religion, politics, etc.)
- Do not whine or beg
- Avoid being argumentative or combative



ULTIMATE GOAL

- Stay alive
- Resist exploitation
- Prepare to escape
- Survive with honor



CHECK ON LEARNING

- Why is establishing a rapport with your captor important?

So the captor sees you as a person rather than a symbol.

- Identify a strategy to use when establishing a rapport?

- (1) Introduce commonalities
- (2) Perform active listening
- (3) Address captors by name (if known)
- (4) Avoid emotionally charged topics (religion, politics, etc.)
- (5) Do not whine or beg
- (6) Avoid being argumentative or combative



ACTIVE SHOOTER / ACTIVE THREATS

- Active Shooters: Individuals who attempt to injure or kill people in confined and populated areas with a firearm, often displaying no pattern in their selection of victims.
- Active Threats: Individuals who conduct the same acts as above but use weapons other than a firearm. These weapons include the following:
 - Knife
 - Axe
 - Other edged weapons, i.e. machete, sword, etc.
 - Motor vehicles
 - Hammers, pipes, or other blunt objects that can kill



INDICATORS OF POTENTIAL VIOLENT BEHAVIOR

Early recognition of a threat can prevent an incident. The following are indicators of potentially violent behavior:

- Aggression or threats towards coworkers.
- Presence of unauthorized weapons.
- Abnormal mood swings or depression, withdrawn behavior, decrease in hygiene, paranoia, increased use of alcohol or drugs.
- Suicidal remarks or comments about “putting things in order.”
- Repeated violations of policies, regulations, or laws.
- Talk of severe financial problems.



ACTIVE SHOOTER/THREAT RESPONSES

Responses include the following:

- . Evacuate
- . Shelter in place
- . Take action against the Shooter/Threat
- . **The easiest way to remember is:**
 - . Run
 - . Hide
 - . Fight



EVACUATE (RUN)

- Have an escape route and plan in mind.
- Evacuate regardless of whether others agree to follow.
- Leave your belongings behind.
- Help others escape, if possible.
- Keep your hands visible.
- Follow the instructions of security personnel (if on scene.)
- Do not attempt to move wounded people.
- Call emergency personnel when you are safe.



SHELTER IN PLACE (HIDE)

- Get behind cover and concealment.
- Lock and block the door.
- Hide behind large items.
- Remain quiet and calm.
- Turn cell phone to mute.
- Call 911, speak if you can or leave the line open.



TAKE ACTION (FIGHT)

- As a last resort, fight with everything that you have.
- Throw items and strike the subject with any improvised weapons that are available such as –
 - Computer screens
 - Chairs
 - Anything in your vicinity that can cause pain.
- Commit to your actions until the subject is neutralized.



COOPERATE WITH FIRST RESPONDERS

- Remain calm and follow instructions.
- Put down any items in your hands.
- Raise hands and spread your fingers.
- Avoid quick movements.
- Do not cling to emergency personnel.
- Avoid pointing, screaming, or yelling.
- Individuals may be initially restrained, searched, and treated as suspects.



CHECK ON LEARNING

What are the three steps when responding to an active shooter/active threat incident?



Evacuate (Run)

Shelter in Place (Hide)

Take Action (Fight)



CHECK ON LEARNING

What are the DoD Threat Levels?

Low, Moderate, Significant and High



When selecting a hotel room, do you want a room on the first floor?

No, You want to select a room on the 3rd through 7th floor.



SUMMARY

Action: Conduct Antiterrorism (AT) Level I Awareness Training.

- Terrorist Tactics and Operations
- Threat Levels and FPCONs
- Individual Protective Measures
- Detecting Surveillance
- Hostage Survival Techniques
- Active Shooter/Active Threat Response

What are your questions?