Department of the Navy Level I Antiterrorism (AT) Awareness Training

Table of Contents

Introduction and Course Logistics *(Running Time 4:43)*

PAGE 1

Audio: Welcome to the Department of the Navy Level I Antiterrorism (AT) Awareness Training.

On screen:

Department of the Navy
Level I Antiterrorism (AT) Awareness Training

PAGE 2

Audio: If you would like to follow along with a written transcript of this training, you can download a copy by clicking on the Transcript icon located in the lower left corner of the screen, marked by the "T" symbol. You can also download the transcript from the Resources page of this training site. You can access the Resources page by clicking on "Resources" at the top of the screen.

Closed captioning is available for this course and can be activated by clicking on the Closed Captioning icon located in the lower left corner of the screen, marked by the "CC" symbol.

On screen:

(Image of course transcript)

PAGE 3

Audio: Users can access this course via screen reader software. When screen reader mode is enabled, this training course will automatically pause at the end of each screen, allowing time to review all on-screen information before continuing. Detailed instructions on how to take this course with assistive software can be found at the link provided here. You can also access these instructions from the Resources page of this training site.

If you are currently using screen reader software, use the Up and Down arrow keys to activate screen reader mode. Otherwise, click on the "RESUME" button to continue without activating these features.

On screen:

If you do not require assistive software, click here to skip this page.

Users requiring additional assistance can access this course utilizing their screen reader software. This feature is only intended for users who currently have assistive software on their computer.

(Image of "View Screen Reader Instructions" button)

Note: Activating screen reader mode without assistive software will prevent the training from running properly.

(Image of "RESUME" button)

PAGE 4

Audio: Individual training modules will be presented during this course, beginning with an introduction to terrorism. We will then discuss Force Protection Conditions (FPCONs). The next section will introduce you to antiterrorism security in several different situation-based environments. They will be presented in the following modules:

- Antiterrorism Fundamentals;
- Surveillance Detection;
- Insider Threat;
- Security During Off-Duty and Free-Time Activities;
- Air Travel Security;
- Ground Travel Security; and
- Hotel Security.

We will conclude the training with where to report suspicious activity and/or behavior and some final thoughts.

On screen:

Course Structure

- Introduction to Terrorism
- Force Protection Conditions (FPCONs)
- Situation-Based Training
    - Antiterrorism Fundamentals
    - Surveillance Detection
    - Insider Threat
    - Security During Off-Duty/Free-Time Activities
    - Air Travel Security
    - Ground Travel Security
    - Hotel Security
- Conclusion

PAGE 5

Audio: Before we begin the training modules, let's discuss the logistics involved in this web-based training.

To accommodate your work schedule, this training provides the ability for you to log out at any time. Your progress will be saved after each page you view. If you log out in the middle of the training, you will resume the training where you left off the next time you log in.

In order to ensure that you are able to complete the course in its entirety, you must always access the course from the same web browser that you initially selected when you began the course. Do not delete your cookies or clear the browsing history while the course is in progress. This will ensure that the browser will retain your progress if you need to exit the training and return at a later time.

For example, if you are accessing the course using Google Chrome, you must complete the course in its entirety using Google Chrome. If you try to access the course using a different browser, such as Edge, you will not be able to resume where you previously left off.

On screen:

Course Logistics

- You may log out at any time during the training
- When you log back in, you will resume training where you left off
- Always access the course from the same browser
- Do not delete cookies or clear browsing history while course is in progress

PAGE 6

Audio: You must complete each training module in the sequence in which it is presented. However, you will be able to review any previously completed training modules by clicking on "Menu", highlighted here, and then on the training topic.

During the presentation of each training module, you will have the ability to pause the presentation, skip back and replay the training module again. If you review a module that has already been completed, you will also have the ability to skip ahead.

On screen:

Course Logistics

- Each training module must be completed in the sequence in which it is presented
- You can review previously completed training modules
- During each training module, you may pause, go back and start again

PAGE 7

Audio: Before completing a module of instruction, you may be presented with a knowledge check to ensure your understanding of the information presented to you during that module.

At the end of the module of instruction and knowledge check, click on the "NEXT" button to proceed to the next module.

On screen:

Course Logistics

- At the end of each training module, you may be presented with a knowledge check to ensure your understanding of the information presented to you
- Upon completion of the knowledge check, click on the "NEXT" button to proceed to the next training module

PAGE 8

Audio: Upon successful completion of the course, a Certificate of Completion will be provided for you to print out.

On screen:

(Image of sample course completion certificate)

PAGE 9

Audio: As previously mentioned, a Resources page has been created for this web-based training. In addition to a written transcript of the training, this page contains links to references used throughout the training. You can access these references at any time for more information regarding the topics being discussed.

On screen:

(Image of course Resources page)

PAGE 10

Audio: Now that you have a feel for how to navigate through this web-based training, let's begin.

Click on the "NEXT" button to start the first training module, an introduction to terrorism.

On screen:

Coming up next:

Introduction to Terrorism

(Image of "NEXT" button)

Introduction to Terrorism *(Running Time 10:36)*

PAGE 1

Audio: In this module, we will provide an introduction to terrorism.

On screen:

Introduction to Terrorism

PAGE 2

Audio: September 11, 2001 was a horrific day that is forever seared in the Nation's memory. Since that day, the United States has been engaged in a Global War on Terror - a war to protect the Nation's freedoms. The Global War on Terror is being fought by virtually every agency within the U.S. Government. Additionally, friends and allies from all corners of the globe have joined the United States in its efforts.

The world is dangerous and we are at war against an enemy intent on destroying the American way of life. While responding to this real and present danger, we must remain vigilant while executing our responsibilities.

On screen:

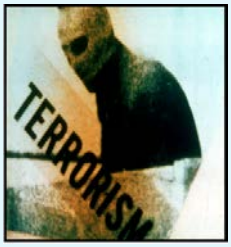
Introduction to Terrorism

PAGE 3

Audio: Terrorism is the calculated use of unlawful violence or threat of unlawful violence to inculcate fear, intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

On screen:

Introduction to Terrorism



The calculated use of violence or the threat of violence to inculcate fear, intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

PAGE 4

Audio: The international terrorist network may exist in the area where you serve and work. Terrorist plots against DoD facilities have been uncovered in such geographically diverse places as Iraq and Washington D.C.

On screen:

Introduction to Terrorism

TERRORIST GROUP: Any organization that uses terrorism in a systematic way to achieve its goals.

PAGE 5

Audio: Stay alert, be aware of your surroundings, and report unusual or suspicious activity. Pay attention to the details of antiterrorism briefings you receive on your locale and when preparing to travel to a new location. Most importantly, make security a part of your routine. Exercise precautions to increase your personal security and the security of your family, colleagues, and organization.

Patience and persistence are the watchwords for defeating terrorism. Terrorists are patient and cunning, and they are waiting for you to let down your guard or settle into a pattern of predictable behavior. Do not be a tempting target. Be vigilant so we may successfully defend America and our freedoms.

On screen:

Introduction to Terrorism

Threat is a real and present danger.

Remain vigilant while executing responsibilities.

International terrorist networks may be present where you work and serve.

Personal safety is important:

- Remain alert
- Be aware of your surroundings
- Report suspicious activity
- Pay attention to antiterrorism briefings
- Make security part of your routine

Do not be a tempting target!

America's effort to fight terrorism includes everyone.

PAGE 6

Audio: There are eight factors you should consider to understand the threat in your environment.

Using these factors, you can be better prepared for the potential risks you face.

1. Are terrorist groups in the area?
2. Are they violent?
3. Do they attack Americans?
4. How active are they?
5. How sophisticated are they?
6. Are they predictable?
7. Will local citizens warn Americans?
8. What tactics and weapons are used?

On screen:

Introduction to Terrorism

There are eight factors you should consider to understand the threat:

1. Are terrorist groups in the area?
2. Are they violent?
3. Do they attack Americans?
4. How active are they?
5. How sophisticated are they?
6. Are they predictable?
7. Will local citizens warn Americans?
8. What tactics and weapons are used?

Weapons seized after a failed terrorist attack.

PAGE 7

Audio: While overseas, it is advisable to conceal your DoD affiliation.

Consider ways you might become a victim of a terrorist attack. Several factors to keep in mind include:

- **Location:** Terrorists may target locations frequented by Americans or U.S. military personnel, such as certain hotels, apartment buildings, public transportation centers, and nightclubs. Avoid possible target locations.
- **Association:** Terrorists may focus on American tourists, personnel associated with the U.S. Government, and individuals who appear to be high-ranking or important. Try to

blend in with the local population. When possible, avoid disclosing your DoD or U.S. Government affiliation.

- **Opportunity:** Terrorists look for "soft targets." Maintain vigilance, practice good personal safety, and alert the proper authorities of suspicious behavior. To attack you, terrorists generally must perceive you, your association, or your location as a target. Do not be an easy target.
- **Predictability:** Terrorists will attempt to exploit routine patterns of behavior.

On screen:

Introduction to Terrorism

Consider ways you might become a victim of a terrorist attack:

- Location: Avoid possible target locations
- Association: Avoid disclosing your DoD or U.S. Government affiliation
- Opportunity: Terrorists look for "soft targets"
- Predictability: Terrorists will attempt to exploit routine patterns of behavior

To attack you, terrorists generally must perceive you, your association, or your location as a target.

While overseas, it is advisable to conceal your DoD affiliation.

PAGE 8

Audio: Terrorists prepare and conduct attacks through predictable steps. Through vigilance, you may be able to recognize preparations for an attack before it is executed. Be alert to unusual behavior that may indicate intelligence gathering, surveillance, collecting materials for an attack, dry runs, and rehearsals.

For example:

- Taking photos or videos of potential targets;
- Writing notes or sketching details about a possible target;
- Showing abnormal attention to details of routine activities and security measures;
- Using false identification;
- Paying cash for items normally bought on credit; and
- Purchasing large quantities of items that could be used as part of an attack (for example, chemicals or cell phones).

If you see something unusual, report it immediately to security officials for further investigation. Make a note of the individual's description and activities, the time of day, and equipment being used.

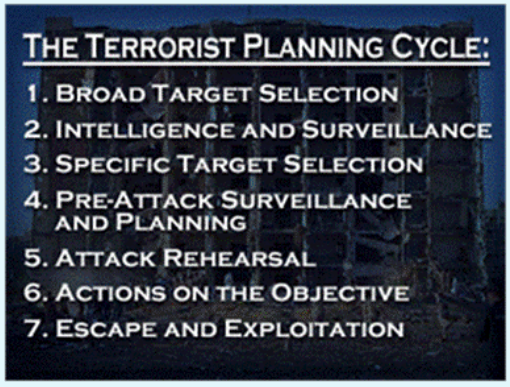
On the following pages, the planning and execution of the attack on the Murrah Federal Building in Oklahoma City illustrates this process. Consider how a vigilant person might have recognized indications of a threat.

On screen:

Terrorist Planning Cycle Overview

Be alert to signs of intelligence gathering, surveillance, collecting materials for attack, and rehearsals:

- Taking photos or videos of potential targets
- Writing notes or sketching
- Showing abnormal attention to details of security measures
- Using false identification
- Paying cash for items normally bought on credit
- Purchasing large quantities of items such as chemicals or cell phones



Terrorists prepare for and conduct attacks through predictable steps.

PAGE 9

Audio: **Phase 1: Broad Target Selection.** During broad target selection, terrorists collect information on numerous targets to evaluate their potential in terms of symbolic value, casualties, infrastructure criticality, or public attention.

Timothy McVeigh wanted to attack a symbol of the federal government, preferably the FBI, Drug Enforcement Administration, or Bureau of Alcohol, Tobacco and Firearms. He identified possible targets such as individual federal employees, their families, and facilities in at least five states.

Phase 2: Intelligence and Surveillance. Vulnerable targets able to meet attack objectives are selected for additional intelligence gathering and surveillance. This effort may occur

quickly or over years, depending upon the target and planning information needed. Terrorists seek to gather detailed information on guard forces, physical layout, personnel routines, and standard operating procedures.

McVeigh performed initial surveillance of the Murrah Federal Building in Oklahoma City, one of his potential targets. He noted the interstate highway allowed easy access and possible escape routes. He also observed indented curbs that permitted vehicles to be parked directly in front of the building.

On screen:

Terrorist Planning Cycle – Phases 1 and 2

Phase 1: Broad Target Selection

- Terrorists collect information on numerous targets
- Evaluate target potential in terms of symbolic value, casualties, infrastructure criticality, or public attention

Phase 2: Intelligence Gathering and Surveillance

- Targets able to meet attack objectives are selected for additional surveillance
- Terrorists seek information on guard forces, physical layout, personnel routines, and standard operating procedures

Murrah Federal Building in Oklahoma City prior to a vehicle bomb attack.

PAGE 10

Audio: **Phase 3: Specific Target Selection.** Specific targets are then identified for attack based on anticipated effects, publicity, consistency with overall objectives, and costs versus benefits of the attack.

McVeigh chose the Murrah Federal Building because he believed the federal agencies represented there were responsible for the incident in Waco, Texas two years earlier. In addition, he assessed the facility as a "soft target," with a good chance of success at low risk. His intent was to kill federal employees and thereby gain media attention.

Phase 4: Pre-Attack Surveillance and Planning. Terrorists may conduct additional surveillance to confirm previous information and gain additional details. During this stage, terrorists will select the method of attack, obtain weapons and equipment, recruit specialized operatives, and design escape routes.

McVeigh recruited Terry Nichols and prepared for the Oklahoma City attack over a six-month period. He acquired materials for a 5,000-pound truck bomb through theft, use of false documents, and paying cash for items normally bought on credit. He also made several trips to the Murrah Federal Building to identify the exact place to park the truck and to select escape routes.

On screen:

Terrorist Planning Cycle – Phases 3 and 4

Phase 3: Specific Target Selection

- Specific targets identified based on anticipated effects, publicity, consistency with objectives, and costs versus benefits

Phase 4: Pre-Attack Surveillance and Planning

- Terrorists may conduct additional surveillance to confirm previous information and gain additional details
- Terrorists select attack method, obtain weapons and equipment, recruit specialized operatives, and design escape routes

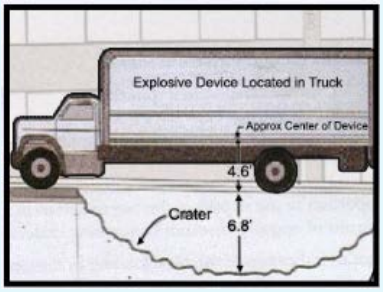


Diagram showing the placement of the vehicle bomb outside the Murrah Federal Building.

PAGE 11

Audio: **Phase 5: Rehearsals.** Terrorists often rehearse the attack scenario to confirm planning assumptions, enhance tactics, and practice escape routes. They may also trigger an incident at the target site to test the reaction of security personnel and first responders.

McVeigh practiced making and detonating bombs in isolated locations. He memorized details of the Murrah Building layout, finalized the sequence of actions for the attack, and practiced responses to law enforcement officers if they were encountered.

Phase 6: Actions on the Objective. Terrorists choose to execute attacks when conditions favor success with the lowest risk. Factors they consider include surprise, choice of time and place, use of diversionary tactics, and ways to impede response measures.

On 19 April 1995, McVeigh parked a rental truck - a 5,000-pound vehicle bomb - in front of the Murrah Federal Building where it could cause the most damage. The date of the bombing was symbolic - the second anniversary of the fire at the Branch Davidian compound in Waco, Texas.

On screen:

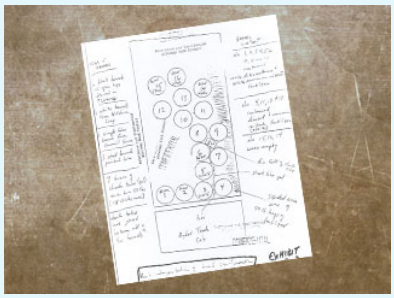
Terrorist Planning Cycle – Phases 5 and 6

Phase 5: Rehearsals

- Terrorists rehearse the attack scenario to confirm planning assumptions, enhance tactics, and practice escape routes
- May also trigger an incident at the target site to test response actions

Phase 6: Actions on the Objective

- Terrorists execute attacks when conditions favor success with the lowest risk
- Factors include surprise, time and place, use of diversionary tactics, and ways to impede response measures



A diagram drawn by McVeigh showing the configuration of the vehicle bomb.

PAGE 12

Audio: **Phase 7: Escape and Exploitation.** Unless an operation is a suicide attack, escape routes are carefully planned and rehearsed. Terrorists may exploit successful attacks by releasing pre-developed statements to the press.

After preparing the bomb for detonation, McVeigh walked away from the scene on a preselected route. To flee Oklahoma City, McVeigh used a get-away car pre-positioned before the attack. McVeigh wanted the world to know that he attacked the Murrah Federal Building because he believed the Federal Government infringed on individual rights of Americans. McVeigh left a file on his sister's computer titled "ATF Read" echoing these sentiments. His get-away car contained anti-government literature, and he subsequently made statements concerning his motivations for the attack.

On screen:

Terrorist Planning Cycle – Phase 7

Phase 7: Escape and Exploitation

- Escape routes are carefully planned and rehearsed
- Terrorists may exploit successful attacks by releasing pre-developed statements to the press

Timothy McVeigh's getaway car after his arrest.

PAGE 13

Audio: This concludes our introduction to terrorism. In the next training module, we will discuss Force Protection Conditions (or FPCONs).

Click on the "NEXT" button to proceed.

On screen:

Coming up next:

Force Protection Conditions (FPCONs)

(Image of "NEXT" button)

Force Protection Conditions (FPCONs) *(Running Time 5:13)*

PAGE 1

Audio: In this module, we will discuss Force Protection Conditions (or FPCONs).

On screen:

Force Protection Conditions (FPCONs)

PAGE 2

Audio: DoD uses a standardized set of terms to describe the terrorism threat level in each country: LOW, MODERATE, SIGNIFICANT, and HIGH. The Defense Intelligence Agency (DIA) sets the terrorism threat level for each country based on analysis of all available information.

The levels are defined as:

- LOW: No terrorist 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 host nation and the 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 its preferred method but has limited operational activity. The operating environment is neutral.
- HIGH: Anti-U.S. terrorists are operationally active and use large casualty-producing attacks as their preferred method of operation. There is a substantial DoD presence and the operating environment favors the terrorist.

Commanders at all levels should use the DIA terrorism threat level plus their own localized threat analyses as a basis for developing plans and programs to protect Service members, civilian employees, family members, facilities, and equipment within their operational areas.

On screen:

Threat Levels

The degree of risk to personnel, facilities, assets or interest.

- **LOW**: No terrorist 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 host nation and the 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**: Anti-U.S. terrorists are operationally active and use large casualty-producing attacks as their preferred method of operation. There is a substantial DoD presence and the operating environment favors the terrorist.

PAGE 3

Audio: U.S. military facilities use a variety of protective measures to reduce vulnerability to terrorist attack. These measures are organized in a system called Force Protection Conditions (or FPCONs). As the threat changes, Commanders change the FPCON to protect personnel.

As the FPCON increases, you can expect to experience delays at gate checks, more detailed inspections, gate closures, and increased guard presence. FPCON CHARLIE and DELTA are very restrictive and rarely used. Normal operations may be reduced or suspended in these cases.

On screen:

Force Protection Conditions

U.S. military facilities use protective measures organized in a system called Force Protection Conditions (FPCONs).

As the threat of attack changes, Commanders change the FPCONs to protect personnel.

FPCONs are organized in five levels with increased protection at each level.

PAGE 4

Audio: FPCONs are organized in five levels with increasing measures of protection: NORMAL, ALPHA, BRAVO, CHARLIE, and DELTA. Commanders adapt protective measures for the local situation, and they can use additional measures and move to a higher FPCON as needed. Measures may also be added randomly to rehearse them, to promote security awareness, and to confuse surveillance by potential threat elements.

FPCON NORMAL applies when a general global threat of possible terrorist activity exists and warrants a routine security posture. At a minimum, access control will be conducted at all DoD installations and facilities.

FPCON ALPHA applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable. The measures in FPCON ALPHA must be capable of being sustained indefinitely.

FPCON BRAVO applies when an increased and more predictable threat of terrorist activity exists. The measures in this FPCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

FPCON CHARLIE applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is likely. Implementation of measures

in this FPCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

FPCON DELTA applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. Normally, this FPCON is declared as a localized condition.

On screen:

Force Protection Conditions

- **NORMAL** - General threat of possible terrorist activity exists but warrants only routine security.
- **ALPHA** - General threat of possible terrorist activity against personnel and installations; nature is unpredictable. Must be capable of being sustained indefinitely.
- **BRAVO** - Applies when increased/more predictable threat activity exists. Must be capable of maintaining measures for weeks.
- **CHARLIE** - Applies when an incident occurs or intel indicates a terrorist action is imminent. Implementation of measures for more than short periods probably will create severe hardship on peacetime activities of the unit.
- **DELTA** - Applies in an area where a terrorist attack has occurred or intel indicates an attack is likely. Normally declared as a localized condition.

PAGE 5

Audio: The intent of the Random Antiterrorism Measure (RAM) program is to present a highly visible, constantly changing security posture that effectively disrupts terrorists' attempts to target DoD assets and personnel.

Commanders must ensure that any RAMs implemented are tailored to the local terrorist threat for command or activity.

RAMs are applied periodically, and at irregular intervals, including hourly, daily, or at other intervals, to help complicate the terrorists' surveillance attempts, and make it difficult for terrorists to predict security force actions accurately.

RAMs are also a means for a Commander to test and rehearse mandatory and supplemental FPCON measures to determine effectiveness or evaluate the security force proficiency during execution of the RAM.

On screen:

Random Antiterrorism Measures (RAMs)

Active Force Protection (FP) measures that change the look of an installation's or facility's FP profile.

- Introduces uncertainty in the perception of the overall FP profile
- Complicates the terrorists' surveillance attempts
- Makes it difficult to predict security force actions accurately
- Enables Commanders to exercise and evaluate FPCON measure effectiveness and proficiency

PAGE 6

Audio: This concludes our discussion on Force Protection Conditions (FPCONs). In the next training module, we will cover situation-based training.

Click on the "NEXT" button to proceed.

On screen:

Coming up next:

Situation-Based Training

(Image of "NEXT" button)

Situation-Based Training: Antiterrorism Fundamentals *(Running Time 5:17)*

PAGE 1

Audio: In this section of the Level I Antiterrorism Awareness Training, we will introduce you to antiterrorism (AT) security in several different environments. These are presented in the following modules:

- Antiterrorism Fundamentals;
- Surveillance Detection;
- Insider Threat;
- Security During Off-Duty and Free-Time Activities;
- Air Travel Security;
- Ground Travel Security; and
- Hotel Security.

Each module will present information for the specific environment, situations in which to apply the knowledge, and a knowledge check with true/false and multiple-choice questions.

This module introduces the four antiterrorism themes found throughout the training.

On screen:

Situation-Based Training: Antiterrorism Fundamentals

AT Fundamentals Introduction

Modules presented:

- Antiterrorism Fundamentals
- Surveillance Detection
- Insider Threat
- Security During Off-Duty/Free-Time Activities
- Air Travel Security
- Ground Travel Security
- Hotel Security

AT Level I themes: Anticipate; Be Vigilant; Don't be a Target; Respond and Report.

PAGE 2

Audio: Anticipating threats, risks, and vulnerabilities is fundamental to antiterrorism security. By doing this, you can make choices that enhance your personal protection.

Ways to do this include:

- Researching prior terrorist attacks;

- Understanding the tactics and techniques used by local terrorist organizations; and
- Knowing the types of targets that have been selected for attack.

Consider consulting these sources of information:

- Local Embassy website;
- State Department travel warnings; and
- Other internet and media resources.

On screen:

Anticipate

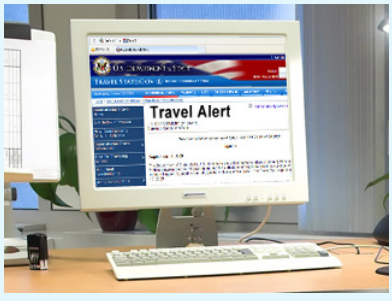
Anticipating threats, risks, and vulnerabilities is fundamental to antiterrorism and personal security.

Ways to do this include:

- Research terrorist activity
- Understand the tactics and techniques
- Know types of targets and locations

Consider consulting these sources:

- Embassy Regional Security Officer
- State Department travel warnings
- Other internet and media resources



Several sources allow you to research threats for yourself.

PAGE 3

Audio: Prior to traveling overseas, consult the Foreign Clearance Guide to make sure you comply with specific requirements for security and coordination. Also, request a threat briefing for the area before departing or upon arriving at your location.

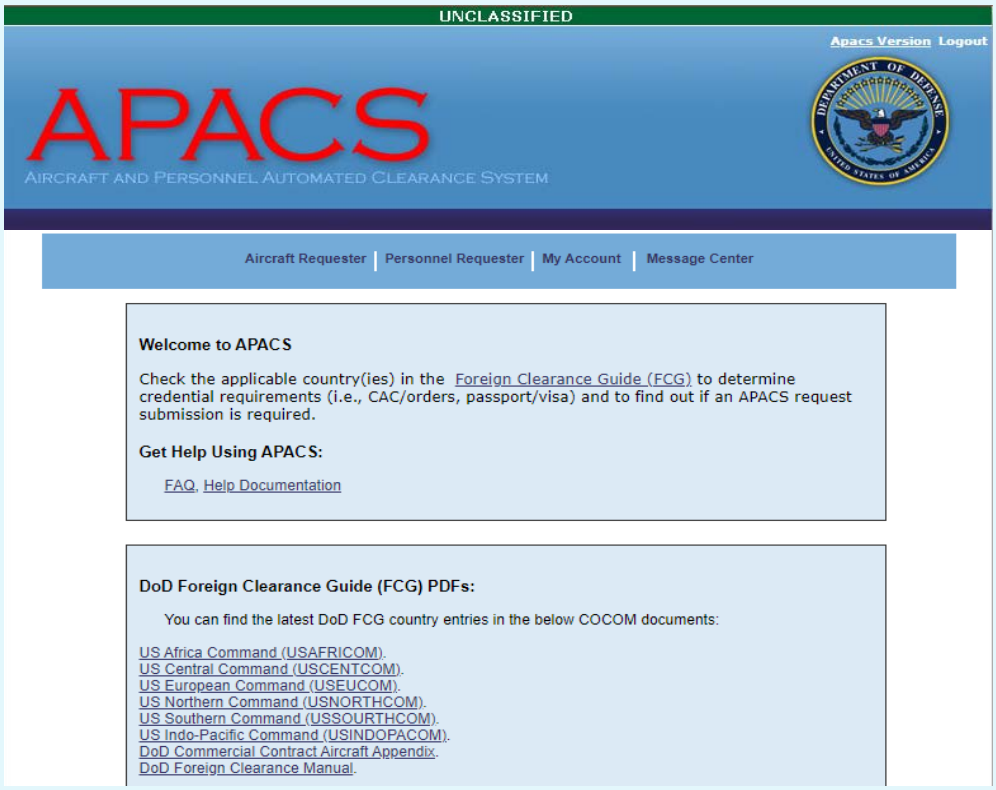
These will help you:

- Determine places you should and should not visit;
- Identify appropriate security measures;
- Recognize possible threats and respond appropriately; and
- Develop security and emergency plans for your home and family.

Planning ahead can enhance your security throughout your foreign travel.

On screen:

Anticipate



https://apacs.milcloud.mil/apacs/login.jsp

PAGE 4

Audio: Vigilance is required to continuously observe your surroundings and recognize suspicious activities. The first step to vigilance is to understand your environment's normal conditions. To do this, try to observe and learn the patterns of routine activities in your area.

When you have an instinct for what is normal, you can more readily recognize things that are suspicious:

- Potential threats, such as items that are out of place, include:
    - Attempted surveillance by persons who are loitering, following you, or are simply in the wrong place;
    - A decrease in activity in an area that may reveal that an attack is imminent;
    - The presence of circumstances that correspond to prior attacks in your area; and
    - The presence of circumstances that correspond to prior criminal activity in your area.

Informed vigilance is fundamental to personal security. Be vigilant and report things that look suspicious to your organization's security officer or to other appropriate authorities.

On screen:

Be Vigilant

Vigilance is required to continuously observe your surroundings and recognize suspicious activities.

Understand your environment's normal conditions.

Knowledge of the normal amplifies abnormal activities.

- Attempted surveillance
- Decrease in activity
- Circumstances that correspond to prior attacks in your area
- Circumstances that correspond to prior criminal activity in your area

Vigilance can thwart many terrorist attacks.

PAGE 5

Audio: Not all threats are predictable or can be recognized in advance. As a result, you should concentrate on not being an easy target for attack. Reduce your exposure by being anonymous and blending in with your surroundings.

- Do not wear clothing or carry items that identify your DoD affiliation;
- Remain low key and do not draw attention to yourself; and
- Avoid places where Americans are known to congregate.

In addition to blending in, try to reduce your vulnerability and exposure:

- Select places with security measures appropriate for the local threat;
- Be unpredictable and vary your routes and times of travel;

- Travel with a friend or in a small group; and
- Use automobiles and residences with adequate security features.

You can greatly increase your personal protection posture by remaining anonymous and reducing your exposure.

On screen:

Don't be a Target

Blend in with your surroundings:

- Do not wear clothing or carry items that identify your DoD affiliation
- Remain low key
- Avoid places where Americans are known to congregate

Reduce your vulnerability and exposure:

- Select places with security
- Be unpredictable
- Travel in a small group
- Use automobiles and residences with adequate security features

DoD affiliation may identify you as a potential target.

PAGE 6

Audio: Report suspicious activities to appropriate authorities immediately. When threatened, respond to protect yourself and others. Specific circumstances may require different responses.

In general:

- Report suspicious activity, do not try to deal with it yourself;
- In threatening situations, take steps to reduce your exposure; and
- Follow the instructions of your DoD sponsor, emergency personnel, and first responders.

Security is a team effort. Try to ensure your actions help trained security personnel do their jobs. You can do this by providing information they need and avoiding becoming a casualty yourself.

Upon arrival at a new location, learn the proper procedures for reporting antiterrorism related information.

Be prepared to report and respond.

On screen:

Report and Respond

Report suspicious activities to appropriate authorities.

- Report suspicious activity, do not try to deal with it yourself
- In threatening situations, take steps to reduce your exposure
- Follow the instructions of emergency personnel and first responders

Security is a team effort.

SEE SOMETHING

SAY SOMETHING

PAGE 7

Audio: Now you will be presented with a knowledge check to test your understanding of the information provided in this module.

On screen:

Knowledge Check

Knowledge Check 1

On screen:

If you identify a possible surveillance attempt, you should try to handle the situation yourself.

A. True

B. **False**

Knowledge Check 2

On screen:

Learning your environment helps you recognize suspicious activity and potential threats.

A. **True**

B. False

Knowledge Check 3

On screen:

Which of the following is ***not*** an Antiterrorism Level I theme?

A. Anticipate

B. Be Vigilant

C. Don't be a Target

D. **Counter-surveillance**

E. Report and Respond

PAGE 8

Audio: This concludes our discussion on antiterrorism fundamentals. In the next training module, we will discuss surveillance detection.

Click on the "NEXT" button to proceed.

On screen:

Coming up next:

Surveillance Detection

(Image of "NEXT" button)

Situation-Based Training: Surveillance Detection *(Running Time 5:08)*

PAGE 1

Audio: In this module, we will discuss surveillance detection.

On screen:

Situation-Based Training: Surveillance Detection

PAGE 2

Audio: Terrorists conduct surveillance to gather information that can be used to create a detailed attack plan. The target of surveillance may be an individual, a facility, or an asset.

Surveillance is conducted against an individual to determine:

- Residential security measures;
- Modes of travel;
- Routes and times of travel;
- Typical behavior; and
- The target's general security awareness.

Surveillance is conducted against a facility or asset to determine:

- General security posture;
- Security standard operating procedures;
- Information on security force shift rotations;
- Physical security weaknesses; and
- Reaction times to emergencies.

Detecting terrorist surveillance is key in preempting a terrorist attack. If you suspect an attempt at surveillance, contact unit or installation security immediately.

On screen:

Surveillance Detection Introduction

Personnel surveillance to determine:

- Residential security measures
- Modes of travel
- Routes and times of travel
- Typical behavior
- The target's security awareness

Facility surveillance to determine:

- General security posture
- Security SOPs
- Information on security force shift rotations
- Physical security weaknesses
- Reaction times to emergencies

Terrorists conduct extensive surveillance against U.S. installations worldwide.

PAGE 3

Audio: You can support security by being vigilant to suspicious activity both inside and outside the perimeter.

First, learn the pattern of things that are normal:

- Recognize legitimate vehicle and uniform markings of host nation support staff;

- Understand the patterns of who should be where on your installation; and
- Learn the local culture.

In conducting surveillance, operatives attempt to blend in with the environment to avoid arousing suspicion. Be vigilant for anything that might be a sign of surveillance:

- People remaining in or coming back to the same general area without a recognizable legitimate reason;
- People preoccupied with a specific area, to include taking pictures, making notes, or drawing sketches;
- Certain civilian vehicles that seem to appear repeatedly;
- Utility and construction workers that do not appear to be performing a specific job; and
- Electronic audio and video devices in unusual places or that are not DoD property.

Learn your environment and recognize suspicious behavior.

On screen:

Surveillance Detection Fundamentals

Be vigilant for anything that might be a sign of surveillance:

- People loitering in the same general area without a recognizable legitimate reason
- People preoccupied with a specific area, to include taking pictures, making notes, or drawing sketches
- Certain civilian vehicles that seem to appear repeatedly
- Utility and construction workers that do not appear to be performing a specific job
- Electronic audio and video devices in unusual places

Installation Entry Control Point

PAGE 4

Audio: Surveillance may be conducted over a long period of time and employ various methods:

Stationary surveillance: A common method in which operatives observe from a fixed location.

- Operatives try to blend in by doing ordinary tasks; and
- Operatives may seek to recruit host nation support personnel or domestic help with access to installations or residences.

Moving surveillance: Conducted on foot or in vehicles, generally in teams.

- Vehicle surveillance may include one or more vehicles;

- Generally uses two or more people, one driving while the others observe; and
- Operatives may not always be behind you; once your routines are learned, they may be in front of you.

Varying your routes and routines can disrupt surveillance attempts.

On screen:

Methods of Surveillance

Surveillance may be conducted over a long period of time and employ various methods:

Stationary surveillance: A common method in which operatives observe from a fixed location.

Moving surveillance: Conducted on foot or in vehicles.

Vary your routes and routines!

Terrorists conduct extensive surveillance against U.S. installations worldwide.

PAGE 5

Audio: Additional surveillance methods include:

Technical surveillance: Uses electronic means to record or gain access to security information.

- May use still and video cameras, including cell phones; and
- May gain access to security information on the Internet.

Casual questioning: Used to elicit security information from approachable personnel.

- Operatives may portray themselves as non-threatening and friendly;

- Terrorists may use unwitting operatives who do not understand the purpose of the information they are asked to gather; and
- Operatives may use members of the opposite sex to gain access to facilities and collect information.

Probing: Terrorists may overtly approach secured areas carrying mock attack devices to determine effectiveness of security procedures.

- Attempts used to gage vigilance and reaction of security personnel.
- Used to desensitize security personnel or produce false alarms that dull effectiveness of security personnel.
- Examples include phone threats, a ruse to gain entry, "accidentally" attempting to smuggle contraband through checkpoints, leaving abandoned packages, vehicles, or suspicious items near a target, and noticeably watching and recording security reaction drills and procedures.

Awareness of terrorist surveillance methods can help you see and respond to surveillance.

On screen:

Methods of Surveillance

Additional surveillance methods include:

Technical surveillance: Uses electronic means to record or gain access to security information.

Casual questioning: Used to elicit security information from approachable personnel.

Probing: May approach secured areas carrying mock attack devices to determine effectiveness of security procedures.

Be aware of terrorist surveillance methods.

Surveillance and recording devices used by terrorists.

PAGE 6

Audio: Review the following surveillance detection situations and determine the correct response.

On screen:

Situations

Situation 1

Audio: You are stationed on a Forward Operating Base in a country of current U.S. military operations. During your time in-country, you have become accustomed to installation routines and the habits of other personnel.

One day, you notice a member of the host nation support staff standing in front of the headquarters building holding a cell phone to his ear. You recognize the individual and know that his duties do not take him to this part of the installation. He is not saying anything, and he is pointing the cell phone's camera lens towards the headquarters building.

You know this is unusual and that you should note the man's activities.

What else should you do?

A. Wait around until he finishes the phone call and then follow him

B. Continue to observe the man to collect as much information as possible

C. Note the man's description

On screen:

You are stationed on a Forward Operating Base in a country of current U.S. military operations. During your time in-country, you have become accustomed to installation routines and the habits of other personnel.

One day, you notice a member of the host nation support staff standing in front of the headquarters building holding a cell phone to his ear. You recognize the individual and know that his duties do not take him to this part of the installation.

He is not saying anything, and he is pointing the cell phone's camera lens towards the headquarters building.

You see a local national photographing the HQ Building.

You know this is unusual and that you should note the man's activities.

What else should you do?

A. Wait around until he finishes the phone call and then follow him

B. Continue to observe the man to collect as much information as possible

C. Note the man's description

Situation 2

Audio: A few days later, you are in your office and a local contract janitor arrives to clean the office. This is routine and members of your office engage him in casual conversation.

However, after saying hello, the janitor loiters around your desk to keep talking. Eventually, he starts asking questions about upcoming deployments.

You know that you should tell him you have no knowledge of the topic.

How do you respond?

A. Politely and quickly end the conversation

B. Ask him why he wants to know the information

C. Try to lead him in conversation to determine what he already knows

On screen:

A few days later, you are in your office and a local contract janitor arrives to clean the office. This is routine and members of your office engage him in casual conversation.

However, after saying hello, the janitor loiters around your desk to keep talking. Eventually, he starts asking questions about upcoming deployments.

You know that you should tell him you have no knowledge of the topic.

The janitor asks probing questions about deployments.

How do you respond?

A. Politely and quickly end the conversation

B. Ask him why he wants to know the information

C. Try to lead him in conversation to determine what he already knows

PAGE 7

Audio: Now you will be presented with a knowledge check to test your understanding of the information provided in this module.

On screen:

Knowledge Check

Knowledge Check 1

On screen:

Surveillance can be performed through either stationary or mobile means.

A. **True**

B. False

Knowledge Check 2

On screen:

Electronic audio and video devices are never used by terrorists for surveillance purposes.

A. True

B. **False**

Knowledge Check 3

On screen:

What is ***not*** a terrorist method of surveillance?

A. Stationary surveillance

B. Moving surveillance

C. Technical surveillance

D. Casual questioning

E. **Breaking and entering to steal valuables**

PAGE 8

Audio: This concludes our discussion on surveillance detection. In the next training module, we will discuss Insider Threat.

Click on the "NEXT" button to proceed.

On screen:

Coming up next:

Insider Threat

(Image of "NEXT" button)

Situation-Based Training: Insider Threat *(Running Time 5:26)*

PAGE 1

Audio: In this module, we will discuss Insider Threat.

On screen:

Situation-Based Training: Insider Threat

PAGE 2

Audio: The Insider Threat is an increasing concern for U.S. officials.

An Insider Threat is a person with authorized access, who uses that access, wittingly or unwittingly, to harm national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities.

Examples of attacks allegedly perpetrated by individuals thought to be loyal to the U.S. include:

- December 2019 active shooter incident at Naval Air Station Pensacola, Florida, and Naval Shipyard Pearl Harbor, Hawaii;
- 2010 leaking of over 500,000 documents concerning operations in Iraq and Afghanistan;
- November 2009 active shooter attack at Fort Hood, Texas; and
- September 2001 anthrax attacks against Government facilities; the perpetrator possibly associated with the U.S. Government.

On screen:

Insider Threat Introduction

An Insider Threat uses access, wittingly or unwittingly, to harm national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities.

Attacks allegedly perpetrated by individuals thought to be loyal to the U.S. include:

- 2019 active shooter incident at Naval Air Station Pensacola, FL, and Naval Shipyard Pearl Harbor, HI
- 2010 leaking of over 500,000 documents concerning operations in Iraq and Afghanistan
- November 2009 active shooter attack at Fort Hood, TX
- September 2001 anthrax attacks against Government facilities; perpetrator possibly associated with the U.S. Government

Hasan

Manning

Snowden

The common threat is usually those with routine access to the information and facility.

PAGE 3

Audio: Motivations for the Insider Threat vary by incident, but common motivations include:

- Desire to further a political or religious agenda;
- Ability to exert power to influence events;
- Perceived injustices against oneself or a minority group;
- The need for excitement;
- The belief that one knows better what U.S. foreign policy should be; and

- The desire to commit suicide.

Individual awareness and active leadership are key defenses to the Insider Threat.

On screen:

Insider Threat Introduction

Motivations for the Insider Threat vary by incident, but common motivations include:

- Desire to further a political or religious agenda
- Ability to exert power to influence events
- Perceived injustices against oneself or a minority group
- The need for excitement
- The belief that one knows better what U.S. foreign policy should be
- The desire to commit suicide

Individual awareness and active leadership are key defenses to the Insider Threat.

Hasan

Manning

Snowden

The common threat is usually those with routine access to the information and facility.

PAGE 4

Audio: There are at least four types of Insider Threats as they relate to antiterrorism.

Terrorism Intended to Coerce or Intimidate: Persons who plot and execute attacks to further the agenda of an extreme ideology.

Mental Instability: Persons that have a mental illness that impairs their judgment and causes them to initiate activities they may not otherwise perform.

Espionage: The divulgence of classified or sensitive information that may result in attacks or provide information on vulnerabilities that facilitate an attack. Motivations may be financial or ideological.

Negligence: Persons that disregard standard security measures that potentially allow the collection of vulnerability-related information or information that could precipitate an attack.

With the exception of negligence, there are four general preconditions for an Insider Threat incident:

- An opportunity to commit the act;
- A motive or need to be satisfied through the act;
- An ability to overcome natural inhibitions to criminal or violent behavior; and
- A trigger that sets activities in motion.

Security personnel are not in the position to recognize and defeat all threats. Therefore, you must be vigilant to a variety of potential threats.

On screen:

Types of Insider Threats

There are at least four types of Insider Threats as they relate to antiterrorism.

- **Terrorism Intended to Coerce or Intimidate:** Persons who plot and execute attacks to further the agenda of an extreme ideology.
- **Mental Instability:** Persons that have a mental illness that impairs their judgment and causes them to initiate activities they may not otherwise perform.
- **Espionage:** The divulgence of classified or sensitive information that may result in attacks or provide information on vulnerabilities that facilitate an attack. Motivations may be financial or ideological.
- **Negligence:** Persons that disregard standard security measures that potentially allow the collection of vulnerability-related information or information that could precipitate an attack.

Preconditions for an incident:

- Opportunity
- Motive
- Ability
- Trigger

In 2010, the National Museum of the Marine Corps was targeted by a drive-by shooter.

PAGE 5

Audio: Early recognition of an Insider Threat can prevent an incident. Pre-attack indicators of terrorism intended to coerce or to intimidate, mostly in pursuit of ideological, religious, or political reasons, include:

- Anti-American statements asserting that U.S. policy and authority is illegitimate;
- Aggression or threats toward coworkers;
- Presence of unauthorized weapons;
- Attempts to communicate with U.S. enemies;
- Associations with known extremist groups;
- Distribution of propaganda materials in support of an extremist position;
- Unfounded allegations of U.S. persecution or prejudice against a minority group or religion; and
- Repeated violation of policies.

If you perceive an immediate violent threat, alert security personnel or law enforcement personnel immediately.

On screen:

Recognizing Political/Religious Extremism

Recognition of an Insider Threat can prevent an incident.

Pre-attack indicators include:

- Anti-American statements asserting that U.S. policy is illegitimate
- Aggression or threats toward coworkers
- Presence of unauthorized weapons
- Attempts to communicate with U.S. enemies
- Associations with known extremist groups
- Distribution of propaganda materials in support of an extremist position
- Allegations of U.S. persecution against a minority group or religion
- Repeated violation of policies

If you perceive an immediate violent threat, alert security personnel or law enforcement personnel immediately.

Humam Khalil Abu-Mulal al-Balawi detonated a suicide bomb at Camp Chapman killing seven CIA operatives.

PAGE 6

Audio: A mentally unstable person may or may not exhibit some of the same behaviors of a prospective terrorist. Indicators of a potentially unstable person often include:

- Abnormal mood swings or depression, withdrawn behavior, decrease in hygiene, paranoia;

- Flashbacks to prior traumatic events;
- Abuse of alcohol or drugs;
- Repeated violation of policies;
- Talk of domestic or financial problems;
- Talk of suicide; and
- Intense anxiety in social situations.

If you witness behavior that might indicate an unstable person, you should alert your supervisor or appropriate medical personnel immediately. Early detection of such behavior can prevent a violent incident and help a person get the help they need.

On screen:

Recognizing Mental Instability

Indicators of a potentially mentally unstable person often include:

- Abnormal mood swings, depression, withdrawn behavior, decrease in hygiene, paranoia
- Flashbacks to prior traumatic events
- Abuse of alcohol or drugs
- Repeated violation of policies
- Talk of domestic or financial problems
- Talk of suicide
- Intense anxiety in social situations

If you witness behavior that might indicate an unstable person, alert your supervisor or appropriate medical personnel immediately.

Abuse of alcohol and drugs is a possible indicator of the Insider Threat.

PAGE 7

Audio: Review the following Insider Threat situations and determine the correct response.

On screen:

Situations

Situation 1

Audio: In light of recent attacks on DoD personnel, you and some friends discuss how to counter the Insider Threat.

What would you do to counter the Insider Threat?

A. Wait for guidance to be issued from your supervisor or local security personnel

B. Learn to recognize indicators that might represent an Insider Threat

C. Carefully monitor the activities of your fellow colleagues

On screen:

In light of recent attacks on DoD personnel, you and some friends discuss how to counter the Insider Threat.

(Image of "NEXT" button)

Knowing indicators of the Insider Threat can help recognize a threatening situation.

What would you do to counter the Insider Threat?

A. Wait for guidance to be issued from your supervisor or local security personnel

B. Learn to recognize indicators that might represent an Insider Threat

C. Carefully monitor the activities of your fellow colleagues

Situation 2

Audio: After reviewing indicators of the Insider Threat, you discuss your response if a potentially mentally unstable person is identified.

You know that indicators of a potentially violent incident should be reported to security personnel or law enforcement personnel immediately, but what do you do if you notice indicators of mental instability, but not necessarily violence?

How do you respond if a potentially mentally unstable person is identified?

A. Try to find them professional help

B. Encourage them to get help from a medical professional

C. Report the behavior you have witnessed to a supervisor

On screen:

After reviewing indicators of the Insider Threat, you discuss your response if a potentially mentally unstable person is identified.

You know that indicators of a potentially violent incident should be reported to security personnel or law enforcement personnel immediately, but what do you do if you notice indicators of mental instability, but not necessarily violence?

Abuse of prescription drugs may indicate an Insider Threat.

How do you respond if a potentially mentally unstable person is identified?

A. Try to find them professional help

B. Encourage them to get help from a medical professional

C. Report the behavior you have witnessed to a supervisor

PAGE 8

Audio: Now you will be presented with a knowledge check to test your understanding of the information provided in this module.

On screen:

Knowledge Check

Knowledge Check 1

On screen:

Knowing indicators of an unstable person can allow you to identify a potential Insider Threat before an incident.

A. **True**

B. False

Knowledge Check 2

On screen:

From an antiterrorism perspective, espionage and security negligence are considered Insider Threats.

A. **True**

B. False

Knowledge Check 3

On screen:

Which of the following is ***not*** an early indicator of a potential Insider Threat?

A. Aggression or threat towards co-workers

B. Presence of unauthorized weapons

C. Abnormal mood swings, depression, and suicidal remarks

D. **A reasonable disagreement with a U.S. Government policy**

E. Anti-American statements asserting that U.S. policy and authority is illegitimate

PAGE 9

Audio: This concludes our discussion on Insider Threat. In the next training module, we will discuss security during off-duty and free-time activities.

Click on the "NEXT" button to proceed.

On screen:

Coming up next:

Security During Off-Duty/Free-Time Activities

(Image of "NEXT" button)

Situation-Based Training: Security During Off-Duty/Free-Time Activities *(Running Time 3:20)*

PAGE 1

Audio: In this module, we will discuss security during off-duty and free-time activities.

On screen:

Situation-Based Training: Security During Off-Duty/Free-Time Activities

PAGE 2

Audio: Off-duty time presents opportunities to visit cultural sites or other civilian establishments. In some environments, terrorists attack these sites because they are vulnerable targets with an exposed population.

Keep risks in mind as you consider visiting civilian facilities such as:

- Places of worship and religious events;
- Shopping centers and marketplaces;
- International hotels with restaurants and recreational facilities;
- Restaurants, coffee shops, and tea houses;
- Night clubs;
- Public transportation hubs; and
- Sporting events.

Outside the protection of your installation or residence, your vulnerability may be increased. Consider your personal security during off-duty activities.

On screen:

Off-Duty Security Introduction

Civilian sites may be more appealing targets than DoD installations.

Examples are:

- Places of worship and religious events
- Common tourist attractions
- International hotels
- Restaurants and coffee shops
- Night clubs
- Public transportation hubs
- Sporting events

Religious and tourist sites may be terrorist targets.

PAGE 3

Audio: Several basic measures can enhance your security when visiting local civilian sites.

These include:

- Travel in a small group;
- Do not draw attention to yourself; instead, conceal your military affiliation and try to blend in;
- Avoid offending local cultural norms with public displays of affection, alcohol, or wearing shorts or skirts;

- Carry emergency phone numbers; and
- Let someone else know where you are going.

Also, it is good to avoid:

- Places where Americans and other Westerners are known to congregate;
- Places of religious significance;
- Political events;
- Establishments that may offend local cultural norms and values; and
- Going out on holidays or anniversaries that may temporarily increase the local threat.

Follow any specific guidance from your activity's antiterrorism officer or the Embassy's Regional Security Officer.

On screen:

Off-Duty Fundamentals

Enhance your personal security by:

- Traveling in a small group
- Not drawing attention to yourself
- Avoiding offending local cultures
- Carrying emergency phone numbers
- Letting someone know your plans

Potential targets include:

- Places Westerners congregate
- Places of religious significance
- Political events
- Establishments that offend locals

Places attracting large groups may be targeted.

PAGE 4

Audio: Public transportation is often a preferred option for getting to off-duty activities. If used, consider these protective measures:

- Select major hubs that might have better security;
- Do not wait in large groups;
- Know your plan and move promptly from one location to the next; and

- Change times and routes for places you visit often.

If taxis are used, consider these guidelines:

- Look for legitimate taxi company markings;
- If a license is viewable, match the photo on the license to the driver;
- Do not always use the same taxi company; and
- Select your own taxi, do not let a stranger select it for you.

Public transportation in foreign countries can be confusing, intimidating, and dangerous, but you can take steps to reduce your vulnerability.

On screen:

Public Transportation

If public transportation is used:

- Select major hubs
- Do not wait in large groups
- Know your plan and move promptly
- Vary your times and routes

If taxis are used, consider these:

- Look for a legitimate taxi company
- Verify the photo on the license
- Vary taxi companies used
- Select your own taxi

Terrorists target public transportation to attack vulnerable passengers.

PAGE 5

Audio: Review the following off-duty situations and determine the correct response.

On screen:

Situations

Situation 1

Audio: You are stationed in an AOR of current U.S. military operations. However, since your specific location is at a lower threat level than other areas, you have been given permission to participate in off-duty activities at some local sites. You and some friends want to see some of the local area.

You know you should follow guidance from your unit and the U.S. Embassy's Regional Security Officer.

What types of locations should you visit?

A. Common tourist attractions

B. Places where Americans and other Westerners congregate since they will probably have better security

C. Places where Americans and other Westerners do not congregate

On screen:

You are stationed in an AOR of current U.S. military operations. However, since your specific location is at a lower threat level than other areas, you have been given permission to participate in off-duty activities at some local sites. You and some friends want to see some of the local area.

You know you should follow guidance from your unit and the U.S. Embassy's Regional Security Officer.

You and your friends want to see a little of the local area.

What types of locations should you visit?

A. Common tourist attractions

B. Places where Americans and other Westerners congregate since they will probably have better security

C. Places where Americans and other Westerners do not congregate

Situation 2

Audio: You and your friends eventually choose a local restaurant that is popular among middle-class locals. When you arrive, you discover the restaurant has outdoor seating on the sidewalk, an indoor seating area away from the street, and a seating area near the entrance. Each area is available.

Where do you sit?

A. Outside seating on the sidewalk

B. The seating area near the entrance

C. The indoor seating area away from the street

On screen:

You and your friends eventually choose a local restaurant that is popular among middle-class locals.

When you arrive, you discover the restaurant has outdoor seating on the sidewalk, an indoor seating area away from the street, and a seating area near the entrance. Each area is available.

You have selected a local restaurant.

Where do you sit?

A. Outside seating on the sidewalk

B. The seating area near the entrance

C. The indoor seating area away from the street

Situation 3

Audio: You and your friends sit at a table in the back of the restaurant away from the street. Feeling a little nervous being out in a new area for the first time, you begin to discuss security.

One member of your party notes that the exits are far away and it would be difficult to get out of the restaurant in an attack. You discuss what you could do if the restaurant comes under a terrorist attack.

You know you should dive for cover immediately.

What else would you do in the event of an attack using firearms?

A. Dive for cover and run for the exit at the first possible opportunity

B. Dive behind something solid and crouch on the floor

C. Dive behind something solid and lie flat on the floor

On screen:

You and your friends sit at a table in the back of the restaurant away from the street. Feeling a little nervous being out in a new area for the first time, you begin to discuss security.

One member of your party notes that the exits are far away and it would be difficult to get out of the restaurant in an attack. You discuss what you could do if the restaurant comes under a terrorist attack.

You discuss how to respond to an active shooter.

You know you should dive for cover immediately.

What else would you do in the event of an attack using firearms?

A. Dive for cover and run for the exit at the first possible opportunity

B. Dive behind something solid and crouch on the floor

C. Dive behind something solid and lie flat on the floor

PAGE 6

Audio: Now you will be presented with a knowledge check to test your understanding of the information provided in this module.

On screen:

Knowledge Check

Knowledge Check 1

On screen:

Your unit or the U.S. Embassy Regional Security Officer may provide a list of places you can and cannot visit.

A. **True**

B. False

Knowledge Check 2

On screen:

It is best to know a little bit about your area so you can recognize unusual activity and behavior.

A. **True**

B. False

Knowledge Check 3

On screen:

What is ***not*** a good selection for where to go during off-duty activities?

A. A place approved by your unit and U.S. Embassy Regional Security Officer

B. **A place of religious association that has caused local controversy**

C. A place not commonly associated with U.S. Service Members

D. Areas away from local political events

E. Establishments that operate in accordance with local norms

PAGE 7

Audio: This concludes our discussion on security during off-duty and free-time activities. In the next training module, we will discuss air travel security.

Click on the "NEXT" button to proceed.

On screen:

Coming up next:

Air Travel Security

(Image of "NEXT" button)

Situation-Based Training: Air Travel Security *(Running Time 3:29)*

PAGE 1

Audio: In this module, we will discuss air travel security.

On screen:

Situation-Based Training: Air Travel Security

PAGE 2

Audio: As a member of the DoD community, you should seek and receive guidance before traveling internationally. Some suggestions here may or may not be relevant to your specific travel situation.

It is generally wise to keep a low profile and not disclose your DoD affiliation:

- Travel with a tourist passport (consult the Foreign Clearance Guide);
- Do not wear clothing with DoD or U.S. symbols or slogans (check with your organization about clothing guidelines);
- Do not include rank or organization on luggage tags;
- Use civilian luggage instead of a military duffle bag; and
- Place any papers with DoD logos or other official documents in a sealed envelope.

When planning your travel, consider the following:

- Travel on U.S. carriers or only on foreign carriers known to have good security; and
- Avoid airports with a history of security problems.

Consider your seat selection. If you have a choice, a window seat reduces your exposure in a skyjacking, but it also reduces your mobility. By thinking through your air travel plans, you can reduce your risk.

On screen:

Reducing Your Exposure during Air Travel

Keep a low profile by:

- Traveling with a tourist passport
- Not wearing clothing with DoD symbols or slogans
- Not including rank or organization on luggage tags
- Using standard civilian luggage instead of military duffle bags
- Placing any papers with DoD logos or other official documents in a sealed envelope

Selecting a window seat reduces your exposure in a skyjacking, but it also reduces your mobility.

Conceal items that show your DoD or Government affiliation.

PAGE 3

Audio: Threats against air travelers occur primarily in two places: at the airport prior to passing security and on the aircraft. When you arrive at an airport, pass through security without delay since all passengers and baggage are screened at that time. To avoid delays, ensure your travel documents are in order and use online check-in options.

While at the airport terminal, be vigilant for:

- Vehicles left unattended at the curbside check-in areas;
- Individuals that appear nervous; and
- Any activity that is out of place in an airport environment.

Report suspicious activity to airport authorities immediately. It is best to wait for your flight in the gate area.

On screen:

Security at the Airport

While at the airport terminal, be vigilant for:

- Vehicles left unattended at the curbside check-in areas
- Individuals that appear nervous
- Any activity that is out of place in an airport environment

Report suspicious activity to airport authorities immediately.

One Team One Fight

PAGE 4

Audio: September 11, 2001 introduced a new tactic to airline skyjacking: use of aircraft as weapons of mass destruction. However, skyjacking is still used to take hostages, and not all skyjackers are intent on suicide.

If your aircraft is skyjacked, you must choose your actions carefully, whether to cooperate or actively resist. Try to understand the skyjackers' intent.

For example:

- Are pilots left in control of the aircraft? This may indicate a desire to land the plane safely.
- Have passengers or crew been physically abused? This may indicate their mindset.
- Are passengers singled out by nationality or religion? This may indicate something about their goal.

Consult your activity's antiterrorism officer for more information about responding to a hostage situation.

On screen:

Skyjacking

If your aircraft is skyjacked, attempt to understand the skyjackers' intent.

- Are pilots left in control of the aircraft? This may indicate a desire to land the plane safely
- Have passengers or crew been physically abused? This may indicate their mindset
- Are passengers singled out by nationality or religion? This may indicate something about their goal

Threats to aircraft come in many forms, and each terrorist may have a different motivation.

PAGE 5

Audio: Review the following air travel situations and determine the correct response.

On screen:

Situations

Situation 1

Audio: You are going TDY to an area of current U.S. military operations. To get to your final destination, you must stay overnight in Istanbul, Turkey. Your overnight stay was uneventful, and the next morning you arrive at the airport to make your connecting flight.

Your taxi stops at the curb close to the doors leading into the airport terminal. As you are getting your bags out of the taxi, you notice an unattended civilian-looking SUV.

You know that Vehicle-Borne Improvised Explosive Devices (VBIEDs) have been used to attack airports in the past and you should not ignore the problem.

What do you do?

A. Look in the windows to see if there is anything suspicious on the floorboards or seat

B. Alert the nearest airport employee or security officer

C. Go into the terminal and try to locate the driver

On screen:

You are going TDY to an area of current U.S. military operations. To get to your final destination, you must stay overnight in Istanbul, Turkey. Your overnight stay was uneventful, and the next morning you arrive at the airport to make your connecting flight.

Your taxi stops at the curb close to the doors leading into the airport terminal. As you are getting your bags out of the taxi, you notice an unattended civilian-looking SUV.

You know that VBIEDs have been used to attack airports in the past and you should not ignore the problem.

You notice an unattended civilian SUV at the curb.

What do you do?

A. Look in the windows to see if there is anything suspicious on the floorboards or seat

B. Alert the nearest airport employee or security officer

C. Go into the terminal and try to locate the driver

Situation 2

Audio: When you arrive at your airline's counter, you notice they have a check-in line specifically for your flight. As you stand in line, the person behind you taps you on the shoulder and asks for a favor. Since you only have one bag to check and he has three, he asks if you can check one of his bags in your name so he will not have to pay a baggage surcharge.

What do you do?

A. Politely say no and note the person's description and any other suspicious behavior.

B. Ask him to open his bag and show you the contents. If it looks okay, check it in under your name.

C. Ask him what's in the bag. If it sounds okay, check it in under your name.

On screen:

When you arrive at your airline's counter, you notice they have a check-in line specifically for your flight. As you stand in line, the person behind you taps you on the shoulder and asks for a favor.

Since you only have one bag to check and he has three, he asks if you can check one of his bags in your name so he will not have to pay a baggage surcharge.

While in line, someone asks you to check a bag for him.

What do you do?

A. Politely say no and note the person's description and any other suspicious behavior.

B. Ask him to open his bag and show you the contents. If it looks okay, check it in under your name.

C. Ask him what's in the bag. If it sounds okay, check it in under your name.

PAGE 6

Audio: Now you will be presented with a knowledge check to test your understanding of the information provided in this module.

On screen:

Knowledge Check

Knowledge Check 1

On screen:

In the event of a skyjacking, you should immediately attempt to subdue the skyjackers.

A. True

B. **False**

Knowledge Check 2

On screen:

The ticketing area is more secure than the area beyond the security checkpoint.

A. True

B. **False**

Knowledge Check 3

On screen:

Since 9/11, which of the following attack methods has ***not*** been attempted against an airport or airline?

A. Small-arms attack

B. VBIED

C. Explosive carried onboard by passenger

D. **Chemical or biological attack**

E. Skyjacking for the purpose of taking hostages

PAGE 7

Audio: This concludes our discussion on air travel security. In the next training module, we will discuss ground travel security.

Click on the "NEXT" button to proceed.

On screen:

Coming up next:

Ground Travel Security

(Image of "NEXT" button)

Situation-Based Training: Ground Travel Security *(Running Time 3:01)*

PAGE 1

Audio: In this module, we will discuss ground travel security.

On screen:

Situation-Based Training: Ground Travel Security

PAGE 2

Audio: A persistent threat exists for DoD Service Members and contractor personnel using ground vehicles in areas of current operations. Traditional threats include sniper attacks, vehicle ambushes, kidnapping, and roadside explosives.

However, in recent years there has been a dramatic increase in the use of Improvised Explosive Devices (IEDs). Terrorists can employ IEDs against ground vehicles with limited risk to themselves while producing many casualties and a dramatic psychological impact.

On screen:

Ground Travel Introduction

For many decades, DoD personnel have had to protect themselves against threats while traveling in vehicles.

Terrorist tactics include:

- Sniper attacks
- Ambushes
- Kidnapping
- Roadside explosives

A Vehicle-Borne IED (VBIED)

PAGE 3

Audio: Keep several measures in mind when considering vehicle security:

- **Prepare adequately** - Keep maps of the local area, a cell phone, and a first aid kit in your car.
- **Ensure your vehicle is well maintained** - A reliable vehicle is good for security and safety. Keep your tires properly inflated and the fuel tank at least half-full.
- **Be vigilant** - When getting out of your car, look around for suspicious activities and individuals.
- **Vary routes** - This makes it harder for terrorists to plan attacks. Do not be a predictable target.
- **Report suspicious behavior** - Be alert to unusual things, such as the absence of people in a marketplace. Alert your leadership and security officials immediately.

On screen:

Ground Travel Introduction

Security and safety measures:

- **Prepare adequately** - Local maps, cell phone, first aid kit
- **Ensure your vehicle is well maintained** - Tires properly inflated and the gas tank at least half-full
- **Be vigilant** - Look around for suspicious activities and individuals
- **Vary routes** - Do not be a predictable target
- **Report suspicious behavior** - If you witness suspicious behavior or possible threats, alert authorities immediately

A U.S. patrol clears the road of Improvised Explosive Devices.

PAGE 4

Audio: Perform vehicle inspections for tampering or sabotage as local conditions warrant.

When you get a new vehicle, inspect it to familiarize yourself with its normal appearance so you can identify potential threats in the future. Inspect it whenever it has been in an unsecured location.

A good vehicle inspection consists of the following:

- **Visual exterior inspection:** Without touching the vehicle, look for any evidence of tampering on the undercarriage and in the wheel wells.
- **Visual interior inspection:** Without touching the vehicle, look through the windows for anything unusual on the seats or floorboards.

- **Complete interior inspection:** Look under the hood, in the trunk, in the glove compartment, behind the gas cap cover, under the seats, in the interior console – anywhere something may be hidden.

You do not need to be an expert to perform a thorough inspection. Vigilance is the key.

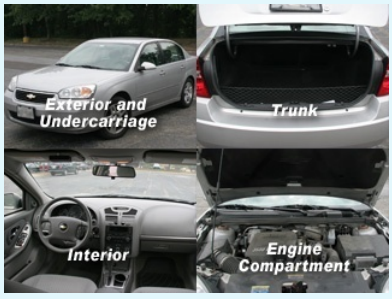
On screen:

Inspecting Your Vehicle

A vehicle inspection consists of the following:

- **Visual exterior inspection:** Look for any evidence of tampering
- **Visual interior inspection:** Look through the windows for anything unusual
- **Complete interior inspection:** Look anywhere something may be hidden

If you believe your vehicle has been tampered with or you see something suspicious, report it to the proper authorities immediately.



Inspect all compartments of your vehicle regularly.

PAGE 5

Audio: Review the following ground travel situation and determine the correct response.

On screen:

Situation

Situation 1

Audio: You are on TDY to a country that is supporting current U.S. operations and you are renting a car at the airport.

You remember that you should select a car typical in the local community and that you should perform an inspection to familiarize yourself with the car.

How often should you perform a vehicle inspection?

A. When you see suspicious activity

B. Every time you leave the vehicle unattended in an unsecured location

C. When the unit you are visiting sends out a warning of possible threats against U.S. personnel

On screen:

On screen:

You are on TDY to a country that is supporting current U.S. operations and you are renting a car at the airport.

You remember that you should select a car typical in the local community and that you should perform an inspection to familiarize yourself with the car.

You perform an initial inspection to familiarize yourself with the car.

How often should you perform a vehicle inspection?

A. When you see suspicious activity

B. Every time you leave the vehicle unattended in an unsecured location

C. When the unit you are visiting sends out a warning of possible threats against U.S. personnel

PAGE 6

Audio: Now you will be presented with a knowledge check to test your understanding of the information provided in this module.

On screen:

Knowledge Check

Knowledge Check 1

On screen:

Varying travel routes can help disrupt the terrorist planning cycle.

A. **True**

B. False

Knowledge Check 2

On screen:

Vehicle inspections begin by looking under the hood and in all compartments.

A. True

B. **False**

Knowledge Check 3

On screen:

When transiting high-threat areas, which of the following is ***not*** a valid security measure?

A. Immediately reporting suspicious behavior

B. Performing a vehicle inspection after your car is left in an unsecured location

C. Choosing a vehicle that blends in with those of the local population

D. **Selecting the quickest and most direct route between two locations**

E. Being vigilant to unusual changes in the local environment

PAGE 7

Audio: This concludes our discussion on ground travel security. In the next training module, we will discuss hotel security.

Click on the "NEXT" button to proceed.

On screen:

Coming up next:

Hotel Security

(Image of "NEXT" button)

Situation-Based Training: Hotel Security *(Running Time 3:53)*

PAGE 1

Audio: In this module, we will discuss hotel security.

On screen:

Situation-Based Training: Hotel Security

PAGE 2

Audio: Hotel security is a significant concern for the U.S. government and host nation governments. In addition to low-level criminal activity, hotels have been targeted with small-arms attacks, Vehicle-Borne Improvised Explosive Devices (VBIEDs), and suicide bombers.

Hotels are attractive targets for terrorists:

- They usually have lighter security than military installations or government buildings;
- They often attract guests who are potential targets, such as affluent local nationals and Western officials and businessmen;
- Terrorists may perceive certain hotels as symbols of American influence or Western economic power; and
- Many hotels employ third-country nationals for house staff and maintenance, further complicating security.

On screen:

Hotel Security

Hotel security is a significant concern for the U.S. government and host nation governments.

Hotels are attractive targets:

- They have lighter security than government installations
- They attract guests who are potential targets
- Terrorists may perceive hotels as symbols of American influence
- Hotels employ third-country nationals for house staff and maintenance

Islamabad Marriott after it was attacked by terrorists.

PAGE 3

Audio: In some overseas areas, you may need to stay in a hotel. The U.S. Embassy or your Command may provide guidance on hotels or direct you to use only pre-approved hotels.

If you have a choice of hotels, consider the following:

- Good standoff from the street to protect from a VBIED;
- Location in a non-violent and low-crime area;
- Solid perimeter, such as a steel fence, solid wall, and vehicle barriers;
- Access control for both persons and vehicles;
- Protection by hotel security personnel or host nation military;
- Location near major roads for use in your daily commute;

- Facilities inside the hotel, such as a restaurant and gym, to limit your need to leave during off-duty hours; and
- Electronic key card security.

On screen:

Selecting a Hotel

When selecting a hotel, consider the following:

- Good standoff from the street
- Location in a low-crime area
- Solid perimeter
- Access control for both persons and vehicles
- Protection by hotel security personnel
- Location near major roads
- Facilities inside the hotel
- Electronic key card security

Islamabad Marriott after it was attacked by terrorists.

PAGE 4

Audio: Selecting a room can be important, though you may not have control of your room assignment. However, if you have the choice, consider the following room preferences:

- 3rd to 5th floors – rooms on the 1st and 2nd floors are easily accessible from the outside, and rooms above the 5th floor are difficult to reach by emergency services;
- A room away from the street can reduce your exposure to a VBIED; and

- Access to fire escapes and emergency evacuation routes.

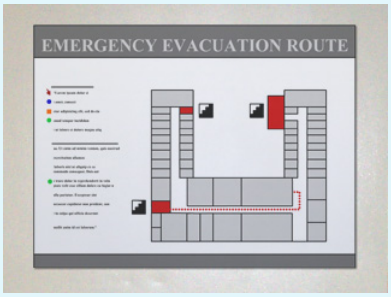
It may be hard to find a room with all these characteristics. If you do not feel your room is safe, ask for another room or consider going to another hotel.

On screen:

Selecting Your Hotel Room

If you have the choice, consider the following room preferences:

- 3rd to 5th floors –1st and 2nd floors are easily accessible from the outside; above the 5th floor is difficult to reach by emergency services
- A room away from the street can reduce your exposure to a VBIED
- Access to fire escapes and emergency evacuation routes



Hotel rooms should be selected with security and safety in mind.

PAGE 5

Audio: Once in your room, inspect it from a security perspective.

Consider these things:

- Functioning locks on all doors and windows;
- Risk of potential access through outside windows or a balcony;
- Location of emergency exits and escape routes;
- How to barricade yourself in your room - is the door solid, and can you move furniture around?
- Peephole to view visitors before opening the door; and
- A working telephone.

Be sure you can call the front desk and call directly to the U.S. Embassy or U.S. military headquarters. If you feel your room is not secure, consider asking for a different room or changing to a new hotel. Changing your room also makes you a more difficult target if someone is specifically interested in you.

On screen:

Inspecting Your Hotel Room

Consider these things:

- Functioning locks on all doors and windows
- Risk of potential access through outside windows or a balcony
- Location of emergency exits and escape routes
- Solid doors to help resist break-ins
- Peephole to view visitors before opening the door
- Operational telephone

Be sure you can call the front desk and call directly to the U.S. Embassy or local installation.

Night latches are common in hotel rooms and should be used.

PAGE 6

Audio: Review the following hotel security situations and determine the correct response.

On screen:

Situations

Situation 1

Audio: You are going TDY to a region with a history of terrorist attacks. On-base accommodations are not available and you have to stay at a local hotel. You get instructions for your travel in accordance with the Foreign Clearance Guide and you receive a list of pre-approved hotels for official travelers.

You have several to choose from. You know you should look for a hotel that is safe and secure.

What should you ask for?

A. A hotel that caters to visiting Westerners and local elites

B. A hotel in a busy part of the city often visited by tourists

C. A hotel with good standoff from the street

On screen:

You are going TDY to a region with a history of terrorist attacks. On-base accommodations are not available and you have to stay at a local hotel. You get instructions for your travel in accordance with the Foreign Clearance Guide and you receive a list of pre-approved hotels for official travelers.

You have several to choose from. You know you should look for a hotel that is safe and secure.

You are looking for a hotel that is safe and secure.

What should you ask for?

A. A hotel that caters to visiting Westerners and local elites

B. A hotel in a busy part of the city often visited by tourists

C. A hotel with good standoff from the street

Situation 2

Audio: At your hotel, you are checking in at the front desk. The receptionist asks if you have room preferences.

You know to ask for a room on the 3rd to 5th floors.

What else should you request?

A. A room with a patio balcony

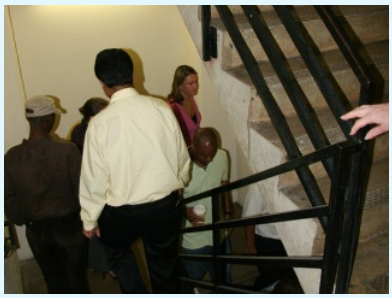
B. A room with metal bars on the windows

C. A room close to emergency exits

On screen:

At your hotel, you are checking in at the front desk. The receptionist asks if you have room preferences.

You know to ask for a room on the 3rd to 5th floors.



You ask for a room on the 3rd through the 5th floor.

What else should you request?

A. A room with a patio balcony

B. A room with metal bars on the windows

C. A room close to emergency exits

Situation 3

Audio: You have been in-country for several days. Every day you leave the hotel at a different time to disrupt terrorist surveillance and planning. You are also alert to learn what is normal behavior in the area.

Most mornings, a man is sitting on a bench across the street from the hotel reading a magazine. When he is still there when you return in the evening, you become suspicious. He is not sitting at a bus stop, and with the traffic noise and fumes, it is not a good place to relax. He seems to be watching the hotel front gate and taking notes. You think this might be an attempt at surveillance.

You know you should alert hotel security to the possible threat.

What else do you do?

A. Report the suspicious activity to U.S. military security personnel.

B. Nothing at the moment. Wait and see if he is outside the hotel again the next day.

C. Go for a walk and cross the street to get a closer look at what the man is doing.

On screen:

You have been in-country for several days. Every day you leave the hotel at a different time to disrupt terrorist surveillance and planning. You are also alert to learn what is normal behavior in the area.

Most mornings, a man is sitting on a bench across the street from the hotel reading a magazine. When he is still there when you return in the evening, you become suspicious. He is not sitting at a bus stop, and with the traffic noise and fumes, it is not a good place to relax. He seems to be watching the hotel front gate and taking notes. You think this might be an attempt at surveillance.

You see a person watching the hotel and taking notes.

You know you should alert hotel security to the possible threat.

What else do you do?

A. Report the suspicious activity to U.S. military security personnel.

B. Nothing at the moment, wait and see if he is outside the hotel again the next day.

C. Go for a walk and cross the street to get a closer look at what the man is doing.

PAGE 7

Audio: Now you will be presented with a knowledge check to test your understanding of the information provided in this module.

On screen:

Knowledge Check

Knowledge Check 1

On screen:

Vehicle and pedestrian access control is a key aspect of hotel security.

A. **True**

B. False

Knowledge Check 2

On screen:

Standoff is important to reduce risk from VBIEDs.

A. **True**

B. False

Knowledge Check 3

On screen:

What is not a physical security feature you should check when inspecting your hotel room?

A. Standoff from the street

B. **Price**

C. Location within the city

D. Presence of hotel security or host nation military personnel

E. A solid physical perimeter

PAGE 8

Audio: This concludes our discussion on hotel security. In the next training module, we will wrap up the course with some final thoughts.

Click on the "NEXT" button to proceed.

On screen:

Coming up next:

Conclusion

(Image of "NEXT" button)

Conclusion *(Running Time 1:23)*

PAGE 1

Audio: In this module, we will conclude the course.

On screen:

Conclusion

PAGE 2

Audio: Report suspicious activities to appropriate authorities immediately. When threatened, respond to protect yourself and others. Specific circumstances may require different responses.

In general:

- Report suspicious activity and/or behavior to one of the points of contact provided; do not try to deal with it yourself.
- Security is everyone's responsibility.

Know your Command's or activity's procedures for reporting suspicious activity. Be prepared to report and respond.

On screen:

SEE SOMETHING, SAY SOMETHING

Report suspicious activity and/or behavior to:

- Eagle Eyes Navy app:

  https://eagleeyes.navy

- Naval Criminal Investigative Service (NCIS)
  - Multiple Threat Alert Center (MTAC) NIPRNET

    https://www.ncis.navy.mil

  - NCIS Tip Line

    https://www.p3tips.com/TipForm.aspx?ID=840&C=&T=

SECURITY IS EVERYONE'S RESPONSIBILITY

PAGE 3

Audio: Terrorism can happen to anyone anywhere.

- Not just the high ranking.
- Not just overseas.

Basic awareness and sound security principles can send terrorists elsewhere.

- Don't be a "soft" target.

Maintain awareness of potential threats in your area and report any suspicious activity immediately.

- Keep family informed and trained.

On screen:

Final Thoughts

Terrorism can happen to anyone anywhere.

- **Not just the high ranking**
- **Not just overseas**

Basic awareness and sound security principles can send terrorists elsewhere.

- **Don't be a "soft" target**

Maintain awareness of potential threats in your area and report any suspicious activity immediately.

- **Keep family informed and trained**





PAGE 4

Audio: This concludes the Department of the Navy Level I Antiterrorism Awareness Training.

Thank you for participating!

Please wait while your record is updated.

On screen:

Thank you for participating!

Please wait while your record is updated.

To receive credit for this training, please contact your local training coordinator.

(The content of external links to non-Federal Agency websites is not endorsed by the Federal Government and is not subject to Federal information quality, privacy, security, and related guidelines.)