Terrorism is a threat to our national security, as well as a criminal act. It is the policy of the United States to use all appropriate means to deter, defeat, and respond to all terrorist attacks against its territories and resources. The Department of Defense (DoD) Antiterrorism (AT) program is a collective, proactive effort focused on the detection and prevention of terrorist attacks against DoD personnel, their families, facilities, installations and associated infrastructure critical to mission accomplishment as well as the preparations to defend against and respond to terrorist incidents.

“The world is a very unpredictable place and we will always have to be flexible to respond to unforeseen crises and events—unforeseen and probably unforeseeable.”

–Eric J. Boswell, Former Assistant Secretary of State.

The lesson objectives are:

- Identify required elements of an AT program, including:
  - Risk Management
  - Planning
  - Training and Exercises
  - Resource application
  - Comprehensive Program Review

Elements of the AT Program

DoD Instruction 2000.16 describes the required elements of an AT program. To understand the relationship between the AT program and an AT plan, think of the program as a collection of ingredients and the plan as the recipe’s detailed instructions.

Commanders and their staff should realize that every available resource must be considered when developing or reviewing an AT program and its associated plan. A typical AT program organization consists of the:

- Installation Commander
- Antiterrorism Officer (ATO)
- Threat Working Group (TWG)
- Antiterrorism Executive Committee (ATEC)
- Antiterrorism Working Group (ATWG)

The AT program is comprised of two phases:

- **Proactive**: Encompasses risk management, planning, resourcing, preventive measures, awareness education, training, and exercising that take place prior to a terrorist incident. During this phase, consideration is given to research and development, implementation of preventive measures, and in-depth installation planning. Commanders and directors must consider the installation, infrastructure, industrial targets, integration of physical assets, force protection (FP), funding requirements, and security forces to detect, assess, delay, and
respond to a threat. Training includes specialized skills proficiency training and exercising plans.

- **Reactive** (crisis management): Includes implementing terrorist incident response and consequence management plans to aid in the resolution of terrorist incidents.

The foundation of the AT program lies with initial assessments that are conducted at the local level:

- **Threat Assessment** is essential; the Commander needs to understand the threat in order to develop an effective AT program.
- **Vulnerability Assessment** goes hand-in-hand with the Threat Assessment. Again, without an accurate Threat Assessment, the Commander will not be aware of the vulnerabilities.
- **Criticality Assessment** determines elements that need protection and are vital to mission accomplishment.

After considering the results of all three assessments, the Commander performs a Risk Assessment (RA). The RA aids in balancing terrorist threats to installation vulnerabilities and the degree of risk that the Commander is willing to accept by not correcting, or perhaps being unable to correct a vulnerability. If any vulnerability is found, the Commander manages the risk by developing a strategy to deter terrorist incidents, employ countermeasures, mitigate the effects of a terrorist incident, and recover from a terrorist incident.

The Commander’s strategy provides direction for developing the rest of the AT program in the following areas:

- Security: Includes operational (OPSEC), personnel, and physical security
- Training
- Exercising
- Reviewing
- Planning

The AT plan is the mechanism for detailing this strategy and coordinating and executing the AT program. Continuous review is essential to ensure the AT program’s improvement and evolution. At a minimum, Threat Assessments, Vulnerability Assessments, Criticality Assessments, and the overall program review will occur annually. DoD Instruction 2000.16 directs that commanders at all levels must conduct annual field and staff training to exercise AT plans. Incident feedback provides valuable insight into program improvement areas.

### Threat Assessment

As part of the AT program, combating terrorism begins with assessing the terrorist threat to DoD personnel and material. The threat of terrorists targeting U.S. Government personnel, facilities, assets, and interests has resulted in the development of an intelligence structure to collect, analyze, and disseminate information about terrorist threats. This structure spans a wide range, from national level organizations to individual installation security.

#### National Level

The National Counterterrorism Center (NCTC) and the National Joint Terrorism Task Force (NJTTF) work together to lead the effort to combat terrorism on a national and international scale.

The NCTC’s mission is to analyze threats, and share and integrate the information. The NCTC provides information on known terrorist groups, individual terrorists, and technical information on topics such as biological or chemical threats.
The NJTTF was established in 2002 to manage the Joint Terrorism Task Force program and is located with the NCTC. The NJTTF supports each task force by sharing intelligence and terrorism threat information and offering guidance and oversight.

**DoD Level**

The Secretary of Defense has assigned the Defense Intelligence Agency (DIA) the responsibility for establishing and maintaining an international all-source terrorism intelligence fusion center. DIA maintains the Combating Terrorism Database (CTDB) and a corresponding Web site called the Combating Terrorism Knowledge Base (CTKB). The DIA also sets the threat level for each country around the world for the DoD.

**Unified Commands**

All Unified Commands have their own supporting joint intelligence centers and intelligence organizations. The J-2 staff draws upon information and analysis resources of the DIA, the Services and other national agency representatives, to include U.S. Embassies in an area of responsibility (AOR), to set a threat level. This threat level may be different than the threat level established by the DIA.

The Secretaries of the Military Departments ensure that the capability exists to receive, evaluate and disseminate all relevant data on terrorist activities, trends, and indicators of an imminent attack. To accomplish this task, each Service Secretary appoints a Service lead agency to monitor foreign intelligence and counterintelligence activities focusing on terrorist groups and terrorist acts. These agencies are:

- **Air Force**: Air Force Office of Special Investigations (AFOSI)
- **Army**: Army Counterintelligence Center (ACIC)
- **Navy**: Navy Criminal Investigative Service Multiple Threat Alert Center (NCIS-MTAC)
- **Marine Corps**: Marine Corps Counterintelligence Center (MCIA)

Each agency establishes, as needed, field intelligence officers on an area basis to collect and disseminate information to Commanders. They are directed to collect information on terrorist threats to DoD personnel, facilities, and assets. Intelligence/counterintelligence staff elements of DoD agencies and commanders shall:

- Report promptly all actual or suspected terrorist incidents, activities, and early warning of terrorist attacks to their immediate Commander, supported activities, Service lead agency, and DIA.
- Initiate and maintain liaison with security police, local military criminal investigative agencies, local intelligence field offices, host nation agencies, and other organizations, elements, and individuals as required.
- Develop and present terrorist threat awareness briefings.

Law enforcement elements of DoD agencies and military commands are responsible for:

- Initiating and maintaining liaison with local intelligence field offices and military criminal investigative organizations
- Investigating criminal activities committed within their jurisdiction to determine whether or not such activities may constitute a terrorist threat to DoD personnel, facilities, material, or other U.S. interests
- Reporting all actual or suspected terrorist incidents or activities to their immediate commander, supported activities, and Service lead agency through established reporting channels
- Maintaining liaison with Federal, host nation, and local law enforcement agencies; and civil and military agencies combating terrorism
In 2007, the eGuardian System was created to share terrorism-related information across federal, state, local, and tribal jurisdictions. The Secretary of the Army has been delegated to the DoD administrator of the eGuardian system and will establish guidance as necessary to ensure that the DoD Components and DoD personnel with access to the eGuardian system receive training in the proper use of and safeguards for the eGuardian system. Access to the eGuardian system is online. DoD personnel whose Law Enforcement responsibilities require access to the eGuardian system must go to the Law Enforcement Enterprise Portal (LEEP) and establish an account.

Contractors must have a sponsorship from a current FBI employee, with an active LEEP account. Initial access to the eGuardian system requires completion of the SAR Line Officer Training video, which addresses standards for reporting and protection of privacy and civil liberties.

The foundation of the threat reporting function demanded by the DoD Combating Terrorism program rests on the shoulders of installation, facility, activity, or unit security officers. These individuals may not be part of the military intelligence community in a formal sense, however, their overall security and force protection responsibilities place them in positions through which quantities of information of potential interest or concern to the intelligence and law enforcement communities pass on a recurring basis. These security officers should:

- Report all actual or suspected terrorist incidents or activities to their immediate Commander, supporting security or military police offices, other supported activities, local intelligence field offices, and local military criminal investigation offices.
- Conduct regular liaison visits with the supporting security or military police office, intelligence field office, and local criminal investigation office.
- Assist in providing terrorist threat awareness training and briefings to all personnel and family members as required by local situations.

Sources of Intelligence Information

Intelligence information for combating terrorism is diverse and includes:

- Open source materials, which are publicly available and can be collected, retained, and stored without special authorization. Examples include news organizations, which are often the first to report major terrorist incidents. They also provide in-depth reports on terrorist individuals or groups, which provide analysts with insights into terrorist group goals, objectives, motivation of terrorist organizations, modes of recruitment, and tactics of attack. Terrorist groups frequently use the media to promote their cause.
- The World Wide Web (WWW) provides terrorists an outlet to spread propaganda, recruit new members, and aid in fundraising. In addition, the web provides information regarding training, training methods, weapons, and weapon usage.
- Criminal information, since terrorist acts are criminal acts, this information is a lucrative source for terrorist intelligence. Established law enforcement liaison channels must be used to obtain such information because collecting, retaining, and disseminating criminal information is regulated.
- Government sources refer to materials collected, analyzed, and disseminated under official auspices. It can be open source or restricted in distribution. Government sources can include:
  - Scientific and technical reports
  - Political and economic reports
  - Crime and terrorism statistics
  - Policy statements
  - Legislation
  - Official correspondence
• Local information can come from any individuals with regional knowledge. A critical element of local information is reporting suspicious activity.

Threat Analysis

Threat analysis is an essential step in identifying the probability of a terrorist attack and results in a threat assessment. Careful threat analysis is required to detect and correctly evaluate pre-incident indicators of a terrorist attack so timely warning messages can be issued. Threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups, which could target a facility. A threat analysis will review the factors of the terrorist group’s:

- **Operational capability**: The acquired, assessed, or demonstrated level of capability for a terrorist group to conduct attacks.
- **Activity**: Determined by examining a terrorist group’s influencing elements, such as presence, suspected surveillance by the group, and cell activity.
- **Intentions**: Stated and/or the actual history of attacking U.S. interests.
- **Operating Environment**: How the overall environment, including political and security considerations, influences a terrorist group’s ability and motivation to conduct an attack.

Threat levels are assigned based on available intelligence and an analytical assessment. The four DoD threat levels are:

- **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.
- **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.
- **Moderate**: Terrorists are present but there are no indications of anti-U.S. activity. The operating environment favors the host nation.
- **Low**: No terrorist group is detected or the terrorist group activity is non-threatening.

Commanders at the installation level task the appropriate organizations under their command to obtain current threat analyses, disseminate the threat information as appropriate, and ensure that the available threat information is used in the development of the threat matrix. The full range of intelligence and counterintelligence capabilities is utilized in support of two distinct and separate Threat Assessments (TAs):

- **Annual TAs**
- **Ongoing local TAs**

**Annual TA**

Commanders shall prepare a TA at least annually for those personnel and assets for which they have AT responsibilities. Whereas the DoD threat analysis focuses on the activities of specific, known terrorist groups, the annual TA seeks to identify the full range of feasible terrorist capabilities that could be used against the installation or its personnel, to include:

- Weapons, to include all likely or feasible weapons of mass destruction (WMD), including chemical and biological threats
- Tactics
- Techniques
- Methods of attack

Preparation of the annual TA requires careful analysis of known local threats, together with estimates of relevant national and transnational threat capabilities. Locally derived, open-source information regarding the availability of weapons and component materials in the area is also necessary in developing the range of threats.
A planning tool for summarizing the threat analysis is a Threat Matrix. The Threat Matrix ensures security and procedural countermeasures are designed to counter specific threats or to mitigate specific vulnerabilities, and that the risk remaining is well understood by Commanders. The Threat Matrix unambiguously establishes the range of specific threat capabilities that are used to analyze vulnerabilities and plan countermeasures that Commanders will use in making risk assessment decisions. In addition, the Defense Threat Reduction Agency (DTRA) performs threat assessments, provides training, and assists in threat reduction planning, particularly against WMD.

<table>
<thead>
<tr>
<th>Threat Capability</th>
<th>Weapon</th>
<th>Delivery Method</th>
<th>Threat Probability</th>
<th>Threat Severity</th>
<th>Threat Priority (Probability x Severity)</th>
<th>Threat Priority (Inside Perimeter)</th>
<th>Threat Priority (Outside Perimeter)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vehicle Bomb</td>
<td>200 lb.</td>
<td>Vehicle (motorcycle, car, truck, boat, plane)</td>
<td>10</td>
<td>5</td>
<td>55</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1,000 lb.</td>
<td></td>
<td>9</td>
<td>7</td>
<td>63</td>
<td>NA</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>20,000 lb.</td>
<td></td>
<td>4</td>
<td>10</td>
<td>40</td>
<td>NA</td>
<td>4</td>
</tr>
<tr>
<td>Sniper</td>
<td>7.62 mm/308 cal.</td>
<td>Sniper</td>
<td>7</td>
<td>1</td>
<td>7</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>Standoff Weapons</td>
<td>Mortar</td>
<td>Hasty Attack</td>
<td>8</td>
<td>3</td>
<td>24</td>
<td>3</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td>RPG</td>
<td>Hasty Attack</td>
<td>5</td>
<td>2</td>
<td>10</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Suicide Bomber</td>
<td>25 lb.</td>
<td>Personal</td>
<td>6</td>
<td>4</td>
<td>24</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>MANPADS</td>
<td>SA7, SA16</td>
<td>Attack against aircraft in arrival or departure</td>
<td>3</td>
<td>6</td>
<td>18</td>
<td>NA</td>
<td>6</td>
</tr>
<tr>
<td>CBRN</td>
<td>Nerve agent/toxic industrial chemical</td>
<td>Deployed upward of event or train derailment</td>
<td>1</td>
<td>9</td>
<td>9</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>CBRN/Toxic Agent</td>
<td>Cave or pit</td>
<td>2</td>
<td>8</td>
<td>16</td>
<td>4</td>
<td>8</td>
</tr>
</tbody>
</table>

**Example of a Threat Matrix**

**Ongoing Assessment**

In addition to preparing an annual TA, Commanders must also continuously assess local threat information so appropriate Force Protection Conditions (FPCONs) can be set. Continuous threat analysis also supports the warning of suspected target facilities or personnel when threats of an immediate nature are identified.

Commanders at all levels shall forward up and down the chain of command all information pertaining to suspected terrorist threats, or acts of terrorism involving DoD personnel or assets for which they have AT responsibilities. The FPCON describes the progressive level of protective measures taken by DoD components in response to terrorist threats. The FPCON system is the principal means through which the Commander applies an operational decision on how to best guard against a terrorist threat and is designed to facilitate inter-service coordination and support for the combating terrorism efforts of DoD components.

**FPCON**
*(See Module 2, Lesson 1 Student Guide for detailed information on the five levels of Force Protection Conditions (FPCONs)).*

Military Commanders and DoD Civilians exercising equivalent authority are responsible for ensuring that subordinates fully understand FPCON declaration procedures and measures. All FPCON mandatory measures for the current level must be implemented in accordance with DoDI 2000.16. Commanders/DoD Civilians may:
- Implement additional FPCON measures on their own authority
- Develop additional measures specifically tailored for site-specific security concerns
- Declare a higher FPCON for their AOR/installation
Subordinate military Commanders or DoD civilians **MAY NOT** lower a FPCON or implement measures that are less rigorous than those appropriate for the declared FPCON.

**FPCON Program Components**

The DoD FPCON Program will use an effects-based model with three principal components:
- Effects
- FPCON levels
- FPCON measures

As threats to DoD elements and personnel increase, commanders raise the FPCON level from NORMAL to ALPHA through DELTA and implement additional FPCON measures to apply the appropriate combination of effects.

**Deter - Commanders:**

1. Demonstrate credible security capabilities to terrorists and other hostile adversaries to convince them that the cost of conducting hostile acts is higher than the perceived benefit.
2. Dissuade terrorists and other hostile adversaries from executing hostile acts on DoD elements and personnel.
3. Influence terrorists and other hostile adversaries to make them perceive their target’s security capabilities are too difficult to overcome; therefore, terrorists and other hostile adversaries stop their attack planning process.

**Detect - Commanders:**

1. Focus on capabilities designed to detect terrorists and other potentially hostile activities or intentions. Emphasis should be on identifying indicators of these activities and intentions.
2. Identify terrorists and other hostile adversaries by employing the combined observation and reporting capabilities of intelligence, security, law enforcement (including information sharing with local and host-nation authorities), and suspicious activity reporting.
3. Identify terrorists or other hostile adversaries in the pre-attack surveillance and planning phase well before they gain access to any potential targets. Detection measures complement deterrence efforts.

**Delay - Commanders:**

1. Focus on proactive and reactive measures to disrupt the planning and execution cycles of terrorists and other hostile adversaries, and hinder their movements in and around their intended targets.

2. Implement actions designed to gain additional time to complete enhanced protective measures by slowing a terrorist’s or other hostile adversary’s planning and movement.

3. Cause terrorists’ or other hostile adversaries’ planning and movement actions to be sufficiently disrupted, diverted, prohibited, or detained to allow commanders to implement enhanced protection measures.

**Deny - Commanders:**

1. Prevent terrorists and other hostile adversaries from achieving their objectives through restricting physical access, limiting freedom of action, restricting access to essential information, and limiting their ability to set conditions for their success.

2. Prevent terrorists and other hostile adversaries from collecting information on and reaching their targets.

3. Implement proactive measures designed to restrict terrorists’ and other hostile adversaries’ physical access to and essential information on DoD elements and personnel.

**Defend - Commanders:**

1. Use proactive and reactive actions to present fortified targets to terrorists and hostile adversaries and provide commanders with the ability to fulfill the obligation to protect DoD elements and personnel against these threats.

2. Ensure that DoD Components have the ability to respond to, contain, and recover from a terrorist attack (or hostile act) and continue to perform critical missions and essential functions.

3. Employ a combination of protection measures that is sufficient to:
   
   a. Fortify targets so that terrorists’ and other hostile actors’ attack means are ineffective.

   b. Employ an armed response force capable of repelling and containing a terrorist attack or hostile act.

   c. Enable DoD elements and personnel to recover from these events.

In determining FPCON, Commanders and Agency/Organization Directors utilize current threat level information in combination with the following tools:

- Warning Reports
- Vulnerability Assessments
- Intelligence Summaries
- Spot Reports
- Law Enforcement information
- Command liaison
- Best judgment
To enhance the overall effectiveness of a given FPCON, unit Commanders develop and implement a Random Antiterrorism Measures (RAM) program as an integral part of their AT program. RAM is the random use of various protective measures normally employed at higher FPCON in order to:

- Rehearse procedures
- Heighten unit awareness
- Frustrate terrorist planning
- IAW DoDI 2000.16, there are mandatory measures at each FPCON

RAM is intended to complement and supplement, but not replace the FPCON. It is one technique of how an installation can apply the principle of unpredictability to deter terrorism.

Advantages of implementing RAM include, but are not limited to:

- Variation in security routines which makes it more difficult for terrorists to target important assets, build detailed descriptions of significant routines, or predict activities by a specific asset or within a targeted facility or installation
- Increased AT awareness for DoD personnel, their dependents, visitors, and neighbors
- Increased alertness among law enforcement, security, and base or facility personnel
- Validates the capability to execute individual measures from higher FPCONs

Vulnerability Assessment

A vulnerability is a situation or circumstance that if left unchanged and taken advantage of by terrorists, may result in the loss of life or damage to mission essential resources. The Commander uses a Vulnerability Assessment (VA) to determine the susceptibility of assets to attack from threats. This assessment provides the answer to the question, “What kind of attack is the asset most/least vulnerable to?” The assessment identifies vulnerabilities that may be exploited by terrorists and suggests options that may eliminate or mitigate those vulnerabilities.

VA Purpose

The purpose of a VA is to provide Commanders with information to assess the potential vulnerabilities of an installation, activity, port, unit, or base by identifying:

- Weaknesses in physical security plans, programs, and structures
- Inefficiencies and diminished effectiveness of personnel practices and procedures relating to security, incident control, incident response, and incident resolution including, but not limited to, law enforcement and security, intelligence, command, communications, medical, and public affairs
- Enhancements in operational procedures during times of peace, mobilization, crisis, and war
- Resource requirements necessary to meet DoD, Service, combatant command, and local security requirements

DoD Instruction 2000.16, Standard 6, “Terrorism Vulnerability Assessment,” requires the heads of DoD components to:

- Establish a Terrorism Vulnerability Assessment process
- Conduct and update Terrorism Vulnerability Assessments at least annually or more frequently if the terrorist threat assessment or mission requirements dictate

DoD has several tools to assist in conducting VAs:

- **MSHARPP**: Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity
- **CARVER**: Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability
VAs should focus on an installation's overarching AT program. These programs should be assessed continuously to avoid complacency and to gain the benefits from other assessments. Periodic assessments are essential due to evolving terrorist threats, changing security technology, developing and implementing alternative concepts of peacetime operations, and changing local conditions.

Information derived from VAs is classified in accordance with the Defense Threat Reduction Agency (DTRA) Security Classification Guide. VAs will normally occur at the installation level. These assessments should consider the range of identified and projected terrorist threats against a specific location or installation personnel, facilities and other assets. The assessment should identify vulnerabilities and solutions for enhanced protection of DoD personnel and resources.

Local Commanders conduct a local VA for facilities, installations, and operating areas within their AOR. The local vulnerability assessment is conducted annually and addresses the broad range of physical threats to the security of personnel and assets.

A Higher Headquarters VA must be performed at least once every 3 years. This assessment ensures unity of AT efforts throughout subordinate commands and is conducted at DoD components, housing areas, facilities, and/or activities at locations and command levels identified as installations. For the purpose of Higher Headquarters VAs, installation is defined as any DoD facility consisting of 300 or more personnel on a daily basis bearing responsibility for emergency response and physical security plans and programs and possessing authority to interact with local non-military or host nation agencies.

A Higher Headquarters VA satisfies the annual requirement for a local VA.

VAs shall assess at a minimum the following functional areas:

- **AT Plans and Programs:** Examines the installations AT program in accordance with the standards as contained in DoDI 2000.16.
- **Counterintelligence, law enforcement liaison, and intelligence support:** These components have the ability to receive threat information and warnings from higher headquarters and local resources, actively collect information on the threat, process that information, and develop a reasonably postulated threat statement of the activity.
- **AT physical security measures:** Determine the unit's ability to protect personnel by detecting or deterring terrorists, and failing that, to protect by delaying or defending against acts of terrorism.
- **Vulnerability to a threat and terrorist incident response measures:** Examines the unit's ability to determine its vulnerabilities against commonly used terrorist weapons and explosive devices, to include WMD.
- **Vulnerability assessments for terrorists' use of WMD:** Assesses the vulnerability of installations, facilities, personnel and family members to terrorist use of WMD, to include the potential use of chemical, biological, nuclear or radiological agents.

Additionally, the VA examines the availability of resources to support plans as written, the frequency and extent to which these plans have been exercised. It will also examine the degree to which plans complement one another and support the assessed unit's ability to identify changes in the terrorist threat, react to threat changes by implementing appropriate AT measures and provide an appropriate response should a terrorist attack occur.

ATOs conduct a VA as a collaborative effort, using key AT Working Group members as the assessment team. At a minimum, the level of expertise and team composition should support the assessment of the functional areas. Team members should have expertise in the following areas:
Vulnerability Matrix

The purpose of the MSHARPP matrix is to analyze likely terrorist targets. Consideration is given to the local threat, likely means of attack available to the enemy, and variables affecting the disposition (e.g., attractiveness to enemy, potential psychological effect on community, etc.) of potential targets. For each asset, values are assigned based on a one to five scale with five being most vulnerable. Once all asset values are tallied, they can be ordered such that the highest score is “most vulnerable” and the lowest score “least vulnerable.”

<table>
<thead>
<tr>
<th>Target</th>
<th>M</th>
<th>S</th>
<th>H</th>
<th>A</th>
<th>R</th>
<th>P</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corps Headquarters</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>23</td>
</tr>
<tr>
<td>Soldier Barracks</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>25</td>
</tr>
<tr>
<td>Communication Center</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>23</td>
</tr>
<tr>
<td>Fuel Storage</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>21</td>
</tr>
<tr>
<td>Helicopter Hangar</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>2</td>
<td>5</td>
<td>4</td>
<td>29</td>
</tr>
<tr>
<td>Weapon Storage</td>
<td>5</td>
<td>6</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>21</td>
</tr>
<tr>
<td>Electric Transformer</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>24</td>
</tr>
</tbody>
</table>

- **Mission**: Focuses on the threat to the situations, activities, capabilities, and resources on an installation that are vulnerable to a terrorist attack. Mission components consist of the equipment, information, facilities, and/or operations or activities that are necessary to accomplish the installation's mission. When assessing points in this area, determine whether or not an attack on mission components shall cause degradation by assessing the component's importance, effect, and recuperability.
- **Symbolism**: Consider whether the target represents, or is perceived by the enemy to represent, a symbol of a targeted group (e.g., symbolic of U.S. military, government, authority, etc.).
- **History**: Do terrorist groups have a history of attacking this type of target? Focus on local targeting history and capabilities.
- **Accessibility**: A target is accessible when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. The four basic stages to consider, when assessing accessibility are: Infiltration from the staging base to the target area, movement from the point of entry to the target or objective, movement to the target’s critical element, and exfiltration.
- **Recognizability**: A target’s recognizability is the degree to which it can be recognized by an operational element and/or intelligence collection and reconnaissance asset under varying conditions.
- **Population**: Addresses two factors: quantity of personnel and their demography. Demography asks the question “who are the targets?”
- **Proximity**: Is the potential target located near other personnel, facilities, or resources that, because of their intrinsic value or “protected” status and a fear of collateral damage, afford it some form of protection (e.g., near national monuments, protected/religious symbols, etc., that the enemy holds in high regard)?
Criticality Assessment

The Criticality Assessment (CA) identifies key assets and infrastructures that support DoD missions, units, or activities and are deemed mission critical by military commanders or civilian agency managers. A CA addresses the impact of the temporary or permanent loss of key assets or infrastructures to the installation and/or unit's ability to perform its mission. It examines costs of recovery and reconstitution, including:

- Time
- Dollars
- Capability
- Infrastructure support

CA Purpose

The purpose of the CA is to examine all assets on an installation and provide a prioritized list based on necessity for mission completion. Do not exclude some assets because they are not physically located on the installation. For example, a telephone switchboard, not located on an installation may be essential to communications if alternative systems are not identified.

The goal of the CA is to determine:

- Vulnerability of installation's key assets
- Whether critical functions can be duplicated under various scenarios
- Time required to duplicate key assets or infrastructure efforts if temporarily or permanently lost
- Priority of response time to key assets, functions, and infrastructures in the event of fire, bombings, or other terrorist attacks

CA Criteria

Determine asset criticality using the CARVER matrix:

- **Criticality**: How rapidly will the impact of asset destruction affect the unit’s essential functions? What percentage of output and essential functions is curtailed by asset damage? Are there substitutes for the output product or service? What is the number of assets, and what is their position in the system or in the complex flow diagram? How critical is the facility to mission accomplishment?

- **Accessibility**: How easily can an enemy gain access to weapons?

- **Recuperability**: How long will it take to repair or replace the asset?

- **Vulnerability**: Is the asset hardened or guarded? Are measures in place to mitigate the threat?

- **Effect**: Will reprisals against allies result? Will national psychological operations themes be contradicted or reinforced? Will evasion be helped or hurt? Will the enemy population be alienated from its government, or will it become supportive of the government? What is the effect on the local population?

- **Recognizability**: Can the enemy recognize the target and its importance?

The purpose of a CARVER Matrix is to determine the criticality of each asset in order to help prioritize them. For each asset, the assessment team will assign values for each criteria based on a scale from one to five. Once all of the asset values are tallied, they can be ordered such that the highest score is “most critical” and the lowest score is “least critical.”
Risk Assessment

The Risk Assessment (RA) is an analysis of the combined Threat, Vulnerability and Criticality assessments, which will assist the commander in making resource allocation decisions to protect people and assets from possible terrorist threats in resource-constrained environments.

The RA outlines the type of information to collect and how to organize and display the information for decision-making. During the RA process, the Commander must consider the elements of threat, asset criticality, and vulnerability to make well-informed decisions to plan pre-incident FPCON measure implementation and post-incident response. If the installation does not have the resident expertise to conduct a RA, the Commander can use a Joint Staff Integrated Vulnerability Assessment (JSIVA). No standard methodology exists for establishing risk levels and their determination will vary based on the commander's judgment. Although this process is subjective, decisions on where to establish the minimum risk can be focused by considering the following:

- What is the installation's mission? (Criticality Assessment)
- What resources are available for AT activities on the installation? (Vulnerability Assessment)
- Where are the nearest available resources that could augment the installation should an incident occur? (Vulnerability Assessment)

JSIVA

The Joint Staff Integrated Vulnerability Assessment teams were formed in 1997 following a DoD task force report on the 1996 attack on Khobar Towers, Saudi Arabia. The report reviewed the adequacy of security at Khobar Towers and the surrounding area as well as force protection findings, resources and coordination of intelligence and antiterrorism countermeasures on a large scale. The task force found that the DoD had no published standards for force protection of fixed facilities. Their recommendations included:

- Establish prescriptive DoD physical security standards;
- Designate a single DoD agency to develop, issue, and inspect compliance with security standards and provide them with sufficient resources to assist field commanders on a worldwide basis with force protection matters, funds, and the authority to manage research and development efforts to enhance force protection and physical security measures.

The Secretary of Defense designated the Chairman, Joint Chiefs of Staff, as the single point-of-contact for force protection programs. DoD guidelines require that each installation have a higher-headquarters antiterrorism and force protection assessment at least every 3 years. The agency also provides education and training assistance so commanders-in-chief and military service chiefs can establish teams and increase their AT and FP knowledge base. The Defense Threat Reduction Agency (DTRA) conducts 80-100 AT Joint Staff Integrated Vulnerability Assessments (JSIVAs) annually at DoD installations worldwide. Five teams determine vulnerabilities and provide options to assist installation commanders in mitigating or overcoming them.

Each eight-person team from the Antiterrorism Assessments Division, J3 Operations Nuclear Assessments, consists of a team leader and military and civilian specialists. Teams spend approximately five days assessing an installation.
• A terrorist options specialist looks at current threats and threat levels, the threat assessment process and operations security. The specialist also assesses observations, actions and attack mechanisms that may be employed by terrorist groups.

• Two security operations specialists collect information through interviews with key physical security and AT/FP personnel. They review operational plans, personal protection procedures and security forces manning, training and equipment.

• A structural engineer interfaces with base engineers and planners, surveys selected structures, reviews architectural and structural drawings and performs quantitative analysis of blast effects to establish effective standoff distances. They also provide a tutorial on the role engineering plays in the installation's overall force protection posture.

• An infrastructure engineer focuses on the installation's supporting infrastructure such as water, power, and communications protection against terrorist incidents. They also determine if there are any potential single-node points of failure.

• An operations readiness specialist focuses on the installation's preparedness to respond appropriately to a terrorist attack employing explosives, chemical, biological, nuclear and radiological weapons. The operations readiness specialist also reviews public affairs, medical, emergency operations center, legal and communications programs.

• Team reports are provided to the installation commander, the joint staff and the appropriate combatant commander or military service chief.

RA Matrix

The RA enables the Commander to prioritize assets based on the calculated risk. It is important to note that this system is not meant to be a precise science. It is one method of quantifying a subjective decision, in order to generally prioritize areas in terms of risk. To complete the matrix, determine each asset to be examined and assess the following factors:

• Attack Means (AM): Method by which an asset would be attacked. Different groups may present several different attack methods based on the weapons they possess and the methods they use. Sample attack means include small arms fire, car/truck bomb, chemical weapons, and biological weapons.

• Criticality

• Vulnerability

• Probability: Likelihood of an attack occurring. Small arms fire and car/truck bomb attacks are more likely to occur than the use of WMD. A scale of 1 to 10 can be used to assess the levels of probability:
  o High: 9-10
  o Significant: 6-8
  o Moderate: 3-5
  o Low: 1-2

The end product of a RA is the identification of areas and assets that are vulnerable to the identified attack means. Based on information developed from all Assessments (Threat, Vulnerability, Criticality, and Risk), the Commander will make a decision on how best to employ given resources and FP measures to deter, mitigate, or prepare for a terrorist attack.
Knowledge Check

Try answering the following questions.

1. A typical AT program organization consists of the following members:
   a. The ATO
   b. The installation military police
   c. Counterintelligence representation
   d. All of the above

2. The initial assessments that set the foundation of the AT program include:
   a. Security
   b. Vulnerability
   c. Criticality
   d. Threat

3. The Secretary of the DoD has assigned the following agency the responsibility for establishing and maintaining an all-source terrorism intelligence fusion center:
   a. IICT
   b. DIA
   c. CCB
   d. Unified Commands

4. To accomplish the task of receiving, evaluating and disseminating all relevant data on terrorist activities, intelligence staff elements of DoD agencies shall:
   a. Develop and present terrorist threat awareness briefings
   b. Investigate criminal activities committed within their jurisdiction
   c. Initiate and maintain liaison with security police
   d. Maintain an all-source intelligence fusion center

5. Threat analysis:
   a. Consists of four threat levels: high, significant, moderate, and low
   b. Is an essential step in identifying the probability of a terrorist attack
   c. Is a continual process of compiling and examining all information concerning potential terrorist activities
   d. Results in a TA

6. The Threat Matrix:
   a. Is a planning tool used to summarize the threat analysis
   b. Ensures that the risk remaining is well understood by Commanders making risk acceptance decisions
   c. Establishes the range of specific threat capabilities for analyzing vulnerabilities and planning countermeasures
   d. A comparison of threat, vulnerability, and criticality assessments

7. Which of the following statements are true?
   a. Commanders may lower an FPCON.
   b. Commanders may raise an FPCON
   c. Commanders may implement additional FPCON measures
   d. Commanders set the FPCON

Choose the correct definition for each effect

8. Deter:
   a. Identify indicators of hostile actions
b. Disrupt planning and execution cycle of terrorists
   c. **Dissuade terrorists from executing hostile attacks**
   d. Respond, contain, and recover from a terrorist attack

9. Deny:
   a. Identify indicators of hostile actions
   b. **Prevent terrorists’ from achieving objectives**
   c. Respond, contain, and recover from a terrorist attack
   d. Identify indicators of hostile actions

10. RAM:
    a. Replaces a current FPCON
    b. **Complements an FPCON**
    c. **Supplements an FPCON**
    d. **Is a technique used to deter terrorism**

10. The Vulnerability Assessment:
    a. **Identifies assets susceptible to terrorist attack**
    b. **Identifies diminished effectiveness of personnel security practices**
    c. Is a planning tool to assess service-wide vulnerabilities
    d. **Suggests options that may mitigate vulnerabilities**

11. Which of the following statement(s) are true?
    a. **VAs will normally occur at the installation level**
    b. **The VA should identify the threats and solutions for enhanced protection of DoD resources**
    c. **The local VA is conducted annually**
    d. A Higher Headquarters VA does not satisfy the annual requirement of a local VA

12. A common tool used to assist with conducting VAs is the:
    a. Threat Matrix
    b. MSHARPP
    c. AT plan
    d. AT program

13. Which of the following statement(s) are true?
    a. **The CA identifies key assets that are deemed mission critical**
    b. The purpose of the CA is to discard any unnecessary assets
    c. **The CA determines whether critical functions can be duplicated under various scenarios**
    d. **The CARVER Matrix assists with prioritizing assets**

14. Which of the following statement(s) are true?
    a. **The elements of threat, asset criticality, and vulnerability must be considered to make well-informed decisions during a RA**
    b. A standard methodology exists for establishing risk levels
    c. **Risk is based on the value of the asset in relation to the threats and vulnerabilities**
    d. **RAs assist the Installation Commander in making resources allocation decisions**

**Lesson Conclusion**

In this lesson, you learned about the required components of an AT Program, including the Threat Assessment, Vulnerability Assessment, Criticality Assessment, and the Risk Assessment.
Lesson 2: Physical Security Considerations

Lesson Introduction

The backbone of the DoD Antiterrorism effort lies in the physical security systems installed in and around DoD installations and facilities. The facilities, equipment, and security forces are the first lines of defense against terrorist attacks.

The lesson objectives are:

- Identify the policies, threats, and measures associated with a physical security system
- Describe the functional requirements of a physical security system
- Determine the physical security measures for an installation
- List the wide range of forms used as installation perimeter barriers
- Analyze and select appropriate vehicle barriers
- Explain how to control vehicle access to an installation

Physical Security System Introduction

DoD 5200.8-R addresses the physical security of personnel, installations, operations, and assets. Assets generally describe buildings, modes of transport (ground, air, and sea), personnel, and smaller objects (i.e., packages, suitcases, and equipment) of DoD Components. The objectives of this regulation are to establish a general policy for the security of personnel, installations, military operations, and certain assets, provide realistic guidance, general procedures, and the necessary flexibility for commanders to protect personnel, installations, operations, and assets from typical threats, and to reduce the loss, theft, or diversion of, and damage to DoD assets, ensuring that war fighting capability is maintained.

The physical security system is defined as that part of security concerned with active and passive measures, designed to prevent unauthorized access to personnel, equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage, and theft. Physical security is a primary command responsibility.

Active and passive measures are standards used to define acceptable or unacceptable security measures, not based on fixed construction standards, but reflective of the variable nature of physical security threats to DoD assets, the dynamic character of the DoD force structure, the distribution of forces and assets among widely distributed DoD installations, and the different DoD component activities.

Threats to Physical Security

Physical security systems provide the means to counter threats during peacetime, transition to war, and in wartime. Effective measures must be designed and implemented to counter the following threats:

- Foreign intelligence entities
- Paramilitary forces
- Terrorists and saboteurs
- Criminals
- Protest groups, and
- Disaffected persons - individuals who resort to violent attacks against DoD assets and are motivated by personal anger, not politics.

AT plans should relate the terrorist threats and the effects of potential terrorist attacks on DoD assets to requirements for physical security equipment, protective designs for
structures and installations, security forces, training, local, or host government support, and other facets of an effective AT program.

Physical Security Measures

Physical security measures are a combination of active or passive systems, devices, and security personnel used to protect a security interest from possible threats. Measures include:

- Security forces and owner or user personnel
- Military working dogs
- Physical barriers, facility hardening, and active delay or denial systems
- Secure locking systems, containers, and vaults
- Intrusion detection systems (IDS) - Systems that can detect the passage of an object, animal, or person through a sensor. They can be used to detect the presence of intruders within a restricted zone and in a restricted volume of space such as an office, garage, or hangar. They are especially useful within an installation, and can be used in conjunction with perimeter barriers, security zones, and interior barriers to provide detailed information about the location of a potential threat. If the geography and location of an installation do not permit detection of a threat at its periphery, as is the case when DoD facilities occupy only a portion of a commercial office building, then threat detection must occur in close proximity to the protected DoD asset. Under such circumstances, multiple IDS, based on different detection principles, can be employed to provide threat detection and the additional information needed for classification and assessment.
- Assessment or surveillance systems (i.e., closed-circuit television (CCTV) or thermal imagers)
- Protective lighting
- Badging systems, access control devices, material or asset tagging systems, and contraband detection equipment

Incident Response Forces

Another element of physical security systems is the incident response force, responsible for initial incident control and containment, as well as augmentation and more specialized functions in the event of a terrorist incident. Incident response forces have three interrelated but very different functions to perform as part of their role in physical security systems:

- They function as barriers - a security force presence is a visible and often tangible reminder of harm that could befall an intruder who ventures onto a DoD military installation without proper authorization.
- They are an essential element in the IDS - typically, security forces are responsible for making on-the-spot assessments of initial alarms and their judgment will figure prominently in installation responses.
- They are the initial response force, local augmentation forces, and regional/national special capability response forces - security forces are responsible for initial incident control and containment, as well as augmentation and more specialized functions in the event of a terrorist incident.

Components of a Physical Security System

The goal of the physical security system is to deploy security resources to preclude or reduce the potential for sabotage, theft, trespass, terrorism, espionage or other criminal activity. A security system provides the capability to detect, assess, communicate, delay, and respond to an unauthorized entry attempt.
For a physical security system to protect DoD assets, certain security functions must be performed.

**Threat Detection**

The first challenge to a physical security system is its ability to detect the presence of hostile intruders. As a rule, the earlier the detection of threats and the longer the range at which they are detected, the greater the opportunity to protect DoD assets and minimize the impact of terrorist acts against DoD personnel, material, and facilities. Threat detection is accomplished through human, animal or electronic means, and alerts security personnel to possible threats and attempts at unauthorized entry at or shortly after time of occurrence.

Systems can include guards, closed-circuit television, and electro-optical and infrared imaging systems. Challenges to threat detection include:

- **Ambient Weather Conditions** - Can impact the performance of visual surveillance systems, including guards, CCTV, and electro-optical and infrared imaging systems. The performance of all of these systems is light dependent. Smoke, dust, and other obscurants can interfere with the sensitivity of these systems.

- **Area** - The area in which surveillance systems are attempting to operate can affect their sensitivity. For example, surveillance systems that rely on motion for cues to activity work well in rural environments; however, these same systems suffer data overload due to excessive activity in an urban environment and cease to be useful.

- **Environmental Factors** - The location of surveillance system sensors in relationship to other environmental factors can have a dramatic impact on their effectiveness. Systems can be placed on key terrain (hills, ditches, roads) or on fixed man-made barriers (fences, walls, barricades).

- **Location** - The number and variety of surveillance sensors is contingent on the location of initial threat detection. If a threat can be detected at the outer perimeter, additional sensors can be used between the outer and inner perimeter. This aids in the classification and assessment of the threat before the response force is dispatched. If the installation or facility is compact and little distance separates the outer and inner perimeters, then the incident response force must be dispatched almost immediately on detection of an intrusion in order to complete an assessment of the situation.

**Threat Classification and Assessment**

The presence of a threat is usually detected as a result of an alarm. Surveillance systems, including but not limited to, visual surveillance systems and IDS, transmit data to an information-processing center where detection data is assessed. The purpose of such assessments is to determine if the alarm is real or false. If the alarm was real, is the intrusion hostile or benign?

Often, security personnel use CCTV to assist them in their assessment role. CCTVs can also be slaved to the IDS. When a sensor alarm is activated on a slaved system, a CCTV camera is immediately focused on that area for the security guard assessing the IDS.

**Threat Delay**

Threat delay is provided by perimeter, exterior, and interior physical barriers erected or installed to protect the structure. These physical barriers can include fences, gates, walls, windows, doors, locking systems, ceilings, and floors and are evaluated as a system. The effectiveness of a barrier system is measured by the minimum total delay time it provides on any path into the protected area. Delay time is measured from the
time the intruder is detected until the intruder has penetrated all of the barriers, including the time it takes to travel between barriers and the protected area.

Delay of potential threats is essential in:

- Making definitive threat classifications and assessments. Being able to delay intruders at the installation perimeter long enough to classify the threat (e.g., “human”) and assess it (e.g., “not carrying firearms”) may prevent unnecessary injury or loss of life.
- Allowing the response force an opportunity to take up defensive positions to protect DoD assets, defend facilities and personnel, counterattack, and conclude an incident with the arrest and apprehension of the perpetrators. The longer intruders can be kept away from major DoD assets, the greater the opportunity for DoD personnel to terminate the threat without loss or compromise of mission capability.
- Facilitating the successful evacuation of DoD assets from facilities under attack especially for DoD personnel serving in isolated posts.

Threat Response

Threat response begins immediately upon detection. Response activity increases concurrently with threat classification and assessment. The purposes of the physical security system threat responses are to:

- Stop further intrusion by the threat at the greatest distance possible from the protected asset
- Slow the intruder's rate of advance toward the protected asset as much as possible
- Facilitate the evacuation of the protected asset to safe areas, and
- Secure the protected asset, contain the threat preventing additional hostile resources from arriving, prepare to apprehend the threat, and relieve the protected asset

Physical Security Measures

Let's integrate the DoD AT Program with the physical security system requirements to illustrate the application of a generic physical security system to common aspects of DoD installations and facilities.

DoD 5200.8-R emphasizes the need to think of physical security as a system providing security in depth. In some cases, security-in-depth can be obtained by constructing “islands” of extreme or high security within a “sea” of moderate security, referred to as “enclaving.”

Prudence must be exercised when implementing a physical security system. While systems can be designed to meet the most stressful, conceivable physical security threats intruders might attempt, the actual security measures implemented should be selected based on threat, risk, vulnerability, and criticality of assets to be protected. Physical security systems should be flexible enough to accommodate threat changes, criticality of the asset, physical security equipment and/or infrastructure expansion, and budget constraints.

Major considerations for tailoring a security system to an individual installation or facility, at a minimum, include:

- Location - Is the facility on or off Government property? Does the DoD have complete or partial control of what, where, when, and how things are done in the vicinity of the structure? Is the facility located in the middle of the government control area or is it near the perimeter or adjacent to uncontrolled areas?
- Availability and capability of any local military, DoD and/or civilian police and fire/rescue personnel - What are their maximum response times? What type of capabilities do they have (fire power, special equipment, etc.)? How dependable will the outside agencies be? Has
there been any attempt to exercise these combined forces and have the lessons learned been examined?

- Reliability - Does your installation or facility rely on utility service supplied from outside the protected area as a primary source? Are there back-up utility services within the protected area that can be activated in the event outside services fail? Utility considerations are very important, considering a large majority of physical security systems can be affected with a loss of power.

- Access routes in the vicinity of the installation or facility to be protected - Will the routes support response force equipment and vehicles allowing for an effective response? Are there multiple routes to and from the facilities that could hinder response force efforts by allowing adversaries multiple routes of ingress and egress?

- Cost of system security components

- Agreements and Restrictions - Status of Forces agreements or any other host nation or lease restrictions as well as legal considerations related to the safeguarding of DoD assets overseas. Status-of-forces agreements play a vital role in preserving command authority, guaranteeing fair treatment of individual service members, and conserving scarce resources. They define the legal status of U.S. personnel and property in the territory of another nation. The purpose of such an agreement is to set forth rights and responsibilities between the U.S. and the host government on such matters as criminal and civil jurisdiction, wearing of the uniform, carrying of arms, tax and customs relief, entry and exit of personnel and property, and resolving damage claims.

**Physical Security Considerations**

Facilities and structures, whether built new for use by DoD, modified to meet new requirements, or simply occupied without physical security considerations, should meet certain functional security objectives:

- Physical and psychological boundaries (fences, walls, signs) should establish four areas defined as:
  - Perimeter or property boundaries
  - Exterior security zones (e.g., loading docks, building lobbies, and other work areas)
  - Interior security zones (i.e., general work areas for DoD and contracted personnel)
  - Category III or high security (such as restricted or exclusion) areas (which may include weapon storage areas, aircraft parking areas, executive offices, armories, etc.) with increasing security controls beginning at the property boundaries

- Vehicular traffic signs should clearly designate entrances for delivery vehicles as well as vehicles used by visitors and employees

- Control points should be provided near the site boundaries where feasible

- Sidewalks should be designed to direct personnel toward controlled entrances

- All areas should be supervised or secured so unobserved access is not possible

There is a close interaction between an installations physical security design and safety considerations. As a general rule, activities involving the use of hazardous, toxic, or explosive materials should be isolated from all other activities, and should be separated from each other as well:

- Fuel depots, ammunition storage sites, building and ground agricultural chemical handling, and other hazardous sites should be isolated from unrelated activities as well as separated from each other wherever possible.

- Utility service to hazardous, toxic, or explosive materials handling facilities should be redundant and isolated from other utility services to the installation or facility if at all feasible. This will ensure uninterrupted operation of systems essential to maintenance of health and safety and for the annunciation of emergency conditions.

Consolidation of DoD activities at home and abroad creates opportunities to build new facilities at entirely new DoD installations. DoD Instruction 2000.16 mandates Services
and/or Agencies must establish AT guidelines for new construction to counter terrorism threat capabilities. DoD AT Construction Standards provide the minimum construction requirements that will be incorporated into all inhabited new construction and major renovations. The standards also specify the design criteria for incorporating threat-based AT requirements into military construction projects. The physical security surveys should draw attention to specific, pragmatic issues that can affect the utility and costs of providing physical security to DoD personnel and DoD contractors. Be sure to address the following requirements:

- **Topography** - When selecting a site for a facility, consider its location relative to the base perimeter. Maximize the distance between the perimeter fence and developed areas, providing as much open space as possible inside the fence along the base perimeter. Ideally a new site would be located on or near a high point of land to make these buildings less vulnerable to weapons fire. It also makes observation of personnel trying to illegally enter or leave the installation easier.

- **Siting** - The principal structures should be located away from main thoroughfares and provide for the following:
  - 150-foot minimum setback between perimeter and building exterior if possible
  - Sufficient parking space for personnel outside the compound in a secure area within sight of the building and preferably adjacent to the compound
  - Sufficient parking space for visitors near the site, but not on the site itself if deemed necessary, and cleared without providing direct access to the site
  - Sufficient space to permit the construction of a vehicular security control checkpoint, which will allow vehicles to be searched
  - Sufficient space to permit the construction of a pedestrian security checkpoint to check identification, conduct a package or parcel inspection, or process visitors for access to the site, and
  - Sufficient space for construction of an outer perimeter barrier or wall

- **Environment** - Care should be taken when selecting new sites for DoD facilities. Evaluations should be made on many issues, such as the impact of local traffic flow patterns on the new facility, and any known natural hazards associated with the area such as geological faults, flood plains, and mudslide areas should be considered. Avoid areas suspected of severe environmental contamination adjacent to rail yards, locks, dams, or large fossil fuel or nuclear power plants. These types of structures could pose a threat to your facility if a major accident or terrorist incident occurred at a neighboring facility.

### Installation Perimeter Barriers

Installation perimeter barriers are considered the first line of defense in any physical security system and are usually some form of perimeter protection system. General guidelines for perimeter barriers include:

- An unobstructed area or clear zone maintained on both sides and between permanent physical barriers, and
- In addition to fences and walls, waterways, ditches, berms, and barricades can be effective perimeter barriers.

Permanent structures can be used as perimeters around an entire DoD installation, around enclaves within a DoD installation, or around an isolated building used solely to house DoD activities. The most common permanent structures include walls, fences, berms, and ditches.

### Walls and Fences

Walls and fences provide less than 15 seconds of penetration resistance and cannot be relied upon for more than a short delay. Walls and fences are primarily used to accomplish one or more of the following:
• Provide a legal boundary by defining the outermost limit of a protected area
• Assist in controlling and screening authorized entries into a protected area
• Support detection, assessment, and other security functions
• Cause an intruder to make an overt action that will demonstrate intent to penetrate the protected area
• Serve as a ballistic shield against small arms fire, deny visual observation of activities being conducted within the enclosed area, and add an increased deterrence to scaling
• Serve as a "stand-off" barrier to protect a structure from vehicle bomb blast effects, and
• Channel visitors through an opening, providing better access control

When using walls to enhance security, the following considerations must be addressed:
• Walls should be positioned far enough away from other structures such as trees, telephone poles, antenna masts, or adjacent structures that may be used as aids to circumvent the barrier.
• Walls should be built in such a manner that vehicles cannot park immediately adjacent to them, thereby affording potential intruders a platform from which to mount an attack.
• Concertina wire, picket fences, multi-strand razor or barbed wire, or other devices designed to inhibit an intruder's attempt to go over a wall should be secured to the top of the wall.

Fences are frequently used to establish boundaries between the perimeters of an installation and its surrounding area. Fences, particularly at military facilities, are typically standard metal chain link fences used to establish an outer perimeter, but generally provide little delay time for the trained, well-motivated intruder. These types of fences do, however, provide an important psychological barrier for intruders who might seek to penetrate a facility "just for fun." Chain link or woven metal fences can be stiffened and made somewhat more resistant to penetration by vehicles through several techniques, such as installing vertical support posts at 4-foot intervals, and installing aircraft arresting cables parallel to the ground at 12 or 18 inches off the ground level.

Barbed wire and field and wood fencing are often found at major CONUS and OCONUS installations. Similar to the wall, chain link fences can be topped with concertina wire, razor wire, or multiple strands of barbed wire, which are useful in adding to the psychological barrier effect, but are not likely to substantially increase the amount of delay in penetration to the facility.

Berms and Ditches

Berms and ditches are examples of protective barriers that control access and define the physical limits of a facility. In modern military engineering, berm has come to mean the low earthen wall adjacent to a ditch, constructed from the soil displaced from the ditch. Physical security systems employ berms and ditches to exclude hostile vehicles and slow attackers on foot. Security berms are common around military and nuclear facilities to provide blast effect reduction from external blast forces.

Using berms and ditches for force protection fulfills the following functions:
• Defines boundary limits
• Provides a barrier to moving vehicles, and
• Hinders pedestrian movement

Berms can also be used to intercept projectiles and obstruct lines of sight, however, to achieve those objectives the berm must be high enough or may be combined with landscaping or other construction elements, if necessary.
Temporary Barriers

Temporary devices, such as vegetation, portable fencing, and temporary walls can be used as perimeter barriers.

- Vegetation is economical and aesthetically pleasing and blends into the surroundings. It provides a symbolic but practical delineation of the property line. The main disadvantage of using hedges is the time it takes to grow them to sufficient size to provide a barrier and the requirement for constant maintenance.
- Portable fencing can be used as a temporary perimeter to establish a psychological barrier and to channel pedestrian and vehicular movement. Several portable fencing materials are available on the commercial market such as plastic netting, rolled wooden slat and/or support wire fencing. Materials available within DoD that can be used as portable fences are coils made from concertina wire, canvas panels, and plastic sheeting materials supported by tent posts.
- Temporary walls and rigid barriers can be used to establish barriers against high-speed vehicles approaching DoD installations and facilities. They can be installed along approaches within an installation’s boundaries to force vehicles to make tight, slow turns before approaching gates or building entrances. Types of temporary walls/rigid barriers include:
  - Concrete, sand, or water-filled vehicle barriers (Jersey barriers)
  - Concrete or sand filled oil drums
  - Concrete bollards and/or planters, and
  - Steel or steel-reinforced concrete posts

Expedient Perimeter Devices

It may become necessary to establish a quick perimeter for protection and psychological effect usually to channel pedestrian and vehicular movement and assist with threat detection. Expedient perimeters can establish security zones within an installation or facility, thereby facilitating threat identification, classification, and assessment. The following materials can be used to mark a perimeter:

- Painted lines
- Ropes
- Colored plastic tape
- Sandbags
- Barricades
- Saw horses
- Empty oil drums, and
- Jersey wall segments

Vehicle Barriers

In recent years, all U.S. Government agencies and departments have taken active measures to restrict the ability of vehicles carrying explosives to reach government buildings, housing, and personnel. The destruction of the Khobar Towers Complex in Dhahran, Saudi Arabia, in 1996, as well as the bombing of the U.S. Embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, in 1998, effectively sensitized DoD to the need for vehicle barriers to restrict potential threats to critical structures.

Different types of vehicle barriers are used to avert threats directed toward critical structures.

- **Active barriers** require action by personnel or equipment to permit entry. Examples include electric fence gates, pop-up ramps, and movable beams.
• **Passive barriers** rely on bulk or mass and have no moving parts. Such systems typically rely on weight to prevent entry into restricted areas. Examples include sandbags, Jersey barriers, and guardrails along roads.

• **Fixed barriers** are permanently installed, or heavy equipment is required to move or dismantle them. Examples include hydraulically operated rotation or retracting systems, pits, and concrete or steel barriers.

• **Movable barriers** may be relocated. Even though they are movable, they may require heavy equipment or personnel to assist with the relocation. Examples include 55-gallon drums that have been filled, sandbags, or even vehicles.

• **Portable barriers** are similar to the movable systems mentioned but are usually smaller, easier and quicker to move. Examples include ropes, chains, cables, and tire puncture systems.

• **Expedient barriers** are comprised of material or objects normally used for other purposes, such as vehicles, tanks, and bulldozers.

**Design Considerations**

The following considerations are critical to the proper placement of vehicle barriers:

• **Location** - Exact locations vary; however, vehicle barriers should be as far from critical resources as practical. When possible, gates and perimeter boundary fences should be positioned outside of the blast vulnerability area.

• **Aesthetics** - The overall appearance of a vehicle barrier plays an important role in its selection and acceptance. Many companies consider appearance when designing a barrier in an attempt to avoid the “fortress effect.”

• **Safety** - A vehicle barrier system should be respected as a tool capable of wielding deadly force. Care should be taken to avoid accidental activation and the area should be properly posted with warning signs, lighting, bells, or buzzers as needed.

• **Reliability** - Due to the relatively short period of time vehicle barriers have been produced, a reliable long-term track record is not available. Manufacturers did not always envision the operating environments for their machines, which lead to the development of unanticipated problems. This situation is improving with the manufacturer’s willingness to resolve problems and work effectively with those utilizing the barriers.

• **Maintainability** - Ensure that all areas are addressed including training, maintenance schedules, and spare parts.

• **Cost** - When planning the type and placement of vehicle barriers, be sure to take into account the following cost considerations:
  - Active barriers have higher installation and yearly maintenance costs than passive barriers.
  - Minimize the number of access points to the facility, reducing the number of entrances requiring active barriers.
  - Aesthetics can add to the cost of the barrier system. Planters are aesthetic, but maintenance and upkeep add additional annual operating costs.
  - Ancillary expenses need to be considered, such as access road creation, addition of an entry-control station, vehicle inspection area, turnaround lane, and lighting. Barrier installation is also a cost concern:
    - Surface mounted is the lowest cost and quickest installation option
    - Shallow foundation mounting reduces installation complexity, time, materials and corresponding costs
    - Sub Surface mounting can require extensive excavation and the need to work around buried pipes, power lines, and fiber optic communication lines adding to the cost

• **Things to avoid** - When assessing vehicle barrier requirements and options, consider the following:
Avoid installing sunken (underground) barriers unless the excavation can be drained. Water collection will cause corrosion, and freezing weather may incapacitate the system.

Avoid providing vehicle barriers at entrance gates without providing equivalent protection along the perimeter of the protected area.

Avoid expending large amounts of funding for soft protection of the installation perimeter. It is generally more cost-effective to provide heavy protection of individual buildings or zones within the perimeter.

Avoid providing perimeter vehicle barriers that are not patrolled or frequently observed. Most types can be quickly overcome with simple tools or ramps.

Avoid placing guard posts next to barriers.

If separate barriers are used for exits and entrances, avoid controlling only the entrance while leaving the exit barrier open. Require positive control for the exit.

Avoid a long, straightaway road (greater than 460 feet) to a crash-resistant barrier system. Where this cannot be avoided, provide a passive-type barrier maze to slow traffic prior to arrival at the vehicle barrier.

**Vehicle Access Controls**

As a general rule, barriers should be placed outside the installation perimeter or outside an installation interior perimeter. Let’s look at addressing vehicle access to an installation once an individual is past the perimeter barriers.

Vehicle entry points should be restricted and entry-exit points should be kept to a minimum. To maximize traffic flow and security, only two regularly used vehicular entry-exit points are necessary. Both should be similarly constructed and monitored. One should be limited to employees’ cars, and the second should be used by visitors and delivery vehicles. Depending on the size and nature of the facility, a gate for emergency vehicular and pedestrian egress should be installed outside the perimeter to increase the setback of the buildings. In either case, design and placement of bollards or other anti-vehicular devices should be considered in the early planning stages. It does not make sense to have impenetrable gates connected by easily penetrated walls.

The following capabilities are recommended for vehicle access control systems:

- **CCTV** - Should have the capability to display full-facial features of a driver and vehicle characteristics on the monitor at the security control center.
- **Bollards** - Can protect the security booth and gates against a car crash.
- **Sensors** - Activate the gate, detect vehicles approaching and departing the gate, activate a CCTV monitor displaying the gate, and sound an audio alert in the security control center.
- **Signs** - Instruct visitors and employees.
- **Lighting** - Illuminates the gate area and approaches to a higher level than surrounding areas.
- **Electric gates** - Activated by security personnel at either a booth or security control center or by a badge reader located in a convenient place for a driver.
- **Vehicle perimeter access** - Barriers and gates should be controlled by key card or remote operation when the gatehouse is not staffed. An intercom and CCTV camera with low-light and area scan capability should be provided to facilitate communication between the central security office and personnel in vehicles seeking entry when the access point is closed. The access point should be sufficiently illuminated such that all vehicle occupants can be seen via CCTV.
- **Traffic control devices** - Strategically placed traffic control devices to enable queuing, turnaround, and parking.
- **Vehicle bypass control (gate extensions)** - Low, dense shrubbery, fences, and walls.
• Intercom systems - located in a convenient place for a driver to communicate with the
gatehouse and security control center.

All vehicle entry/exit points should be protected against reverse entry and ramming attacks.
• Entry-exit points should be secured with heavy-duty sliding steel, iron, or heavily braced
chain-link gates equipped with a heavy locking device.
• Approaches to all vehicle exit points should be aligned such that high-speed approach
from outside the perimeter is not possible. The goal of such realignment is to ensure that
intruders cannot simply enter the facility by going against the flow of exiting vehicle traffic.
Passive vehicle barriers should be incorporated into the road.
• Passive vehicle barriers can be incorporated into designs to make ramming attacks
difficult. Vehicle perimeter penetration gates can also be designed to be highly resistant
to ramming attacks. Additional vehicle barriers can be installed behind the gates to
provide security-in-depth against such an attack.

Gates not in use should be barricaded to prevent ramming attacks, locked and verified that
the locks can be operated only by security personnel. Emergency gates should be securely
locked and periodically checked. Any lock found inoperable by security personnel should be
removed immediately and a security department lock substituted in its place. Control over
keys is essential for strict access control.

Some of the measures implemented at DoD facilities in response to terrorist threats may
result in significant traffic congestion at vehicle entry gates. Such congestion can be reduced
if storage lanes are included in installation access alignments. During periods of rigorous
vehicle inspection, security personnel can inspect vehicles and their occupants in groups,
and vehicles waiting their turn for inspection can be held in storage lanes adjacent to the
installation.

This approach to vehicle inspection and installation access will ease traffic congestion for
those not seeking access to the DoD installation. It will also place vehicles and their
operators awaiting inspection in an area where they can be monitored for indications of
potentially threatening behavior.

Storage lanes, protected guard positions, and hard points for security guard booths should be
included on plans for revised vehicle access to permit multiple vehicle inspections for
explosives, weapons, or contraband outside the installation perimeter.

A security officer booth should be constructed to control access at the vehicular entry/exit.
For facilities without perimeter walls, the security officer booth should be installed
immediately inside the facility foyer. If justified by the threat, the security officer booth should
be completely protected with reinforced concrete walls, ballistic doors, and windows. The
booth should be equipped with a duress alarm and intercom system, both announcing at the
facility receptionist and security officer's office. The security officer would also be responsible
for complete operation of the vehicle gate. If necessary, package inspection and visitor
screening may be conducted just outside of the perimeter security officer booth. Provisions
for environmental and personal comfort should be considered when designing the booth.

Knowledge Check

Try answering the following questions.

1. The physical security system:
   a. Provides the means to counter threats
   b. Is a primary command responsibility
   c. Is designed to give access to personnel, equipment, and material
d. Is concerned with active and passive measures

2. Which of the following statement(s) are true?
   a. The earlier the detection of threat, the greater the opportunities for force protection.
   b. If a threat is detected, it is initially reported to the Installation Commander.
   c. Ambient weather conditions impact the performance of visual surveillance systems.
   d. Environmental factors play no role in the performance of surveillance systems.

3. Which of the following statement(s) are true?
   a. A threat is assessed in order to determine if an alarm is warranted.
   b. A threat delay is provided by physical barriers.
   c. Responding to a threat secures a protected asset.
   d. Delay time is measured from the time the intruder is detected until he is apprehended by authorities.

4. Physical security systems should be flexible enough to accommodate
   a. Utility services reliability
   b. Equipment costs
   c. Threat changes
   d. Personnel rotation

5. DoD AT Construction Standards:
   a. Provide minimum construction requirements for new construction and major renovations
   b. Specify design criteria for incorporating threat-based AT requirements
   c. Mandate Services and/or Agencies establish AT guidelines for new construction to counter terrorism threat capabilities
   d. All of the above

6. Walls and fences:
   a. Provide complete penetration resistance to intruders
   b. Assist in controlling authorized entries into a protected area
   c. Support detection, assessment, and other security functions
   d. Provide a legal boundary by defining the outermost limit of a protective area

7. Which of the following statement(s) are true?
   a. An active barrier system requires action by personnel or equipment to permit entry.
   b. A passive barrier system relies on its bulk or mass and has no moving parts.
   c. Vehicle barriers should be close to critical resources.
   d. A rope is an example of a movable barrier.

8. Which of the following statement(s) are true?
   a. Vehicle barriers should be placed inside the installation perimeter for access control.
   b. Vehicle entry points to an installation should be restricted.
   c. As part of the access control system, it is recommended to illuminate a gate area with lighting.
   d. Active vehicle barriers can be incorporated into designs to make ramming attacks difficult.
9. When placing vehicle barriers consider:
   a. Safety
   b. Location
   c. Aesthetics
   d. Size

10. Traffic congestion at vehicle entry gates can be reduced if:
    a. During periods of rigorous vehicle inspection, security personnel can choose random cars for inspection.
    b. During periods of rigorous vehicle inspection, security personnel can inspect vehicles and their occupants in groups.
    c. Storage lanes can be included in installation access alignments.
    d. Vehicles waiting their turn for inspection can be held in storage lanes adjacent to the installation.

Lesson Conclusion

In this lesson, you learned about the policies, threats, and measures associated with a physical security system. You learned about the functional requirements of a physical security system, installation perimeter barriers, and how to control vehicle access to an installation.
Lesson 3:  The DoD Antiterrorism Plan

Lesson Introduction

Protecting DoD personnel and assets from acts of terrorism is one of the most complex challenges for all Commanders. Planning to confront this challenge requires a comprehensive, integrated approach and a strong, clear vision of AT Program requirements. AT planning is critical to deterrence, detection, defense, and response to terrorist incidents.

The lesson objectives are:
- Define an AT plan
- State the requirements for an AT plan
- Identify roles and responsibilities in creating an AT plan
- Identify the five paragraphs comprising the recommended AT plan format
- List reasons why exercising the AT plan is important
- Identify three types of exercises used to test an AT plan

AT Plan Overview

The AT plan contains all of the specific measures that need to be taken in order to establish and maintain an AT program. The AT plan should be written from the Service or Agency level down to the Installation level for permanent operations or locations, and incorporated in operation orders for temporary operations or exercises. The AT Plan itself is typically not classified; however, certain Annexes may be classified. Site-specific AT measures, linked to an FPCON and physical security actions, shall be classified “CONFIDENTIAL.” When separated from the AT or Physical Security Plan, specific AT measures linked to an FPCON and site-specific FPCON levels may be downgraded to “FOR OFFICIAL USE ONLY” if appropriate.

The AT plan must address and incorporate, at a minimum, the following requirements:
- **Threat Assessment** - Enables Commanders to judge the risk and consequences of a terrorist attack. This assessment focuses on the full range of known or estimated terrorist capabilities in the Commander's area of responsibility, including weapons of mass destruction (WMD). Commanders annually integrate threat information prepared by the intelligence community, technical information from security and engineer planners, and information from other sources to prepare their assessments.
- **Vulnerability Assessment** - Provides Commanders with a vulnerability-based analysis of an AT program. The Commander uses this assessment to determine the susceptibility of attack by the broad range of terrorist threats against personnel and assets. The result of the assessment provides a basis for determining antiterrorism measures to protect personnel and assets.
- **Criticality Assessment** - Provides Commanders with a prioritized list of assets based on the necessity for completing a mission. This information is then combined with information obtained from the Threat and Vulnerability Assessments to manage risk.
- **Risk Assessment** - Integrates threat, criticality and vulnerability information in order to make conscious and informed decisions to commit resources or enact policies and procedures that mitigate or define risk. This assessment provides the Commander with a clear picture of the current AT posture and identifies those areas that need improvement.
- **AT FPCON Measures** - Actions taken to deter and/or prevent a terrorist(s) from conducting an attack. AT measures assimilate facilities, equipment, trained personnel, and procedures into a comprehensive effort designed to provide optimal AT protection to personnel and assets. The objective is to ensure an integrated approach to terrorist threats. Well-designed AT measures direct actions that ensure threat detection, assessment, delay, denial, and notification. AT measures should include provisions for the use of physical structures, physical security equipment, chemical-biological-nuclear-radiological-explosive detection and
protection equipment, RAMs, response forces, and other emergency measures. AT measures should be scalable and proportional to increases in the local threat and/or operational capability.

- **Terrorist Incident Response Measures** - Limit the effects and the number of casualties resulting from a terrorist attack.
- **Terrorist Consequence Management Measures** - Include emergency response and disaster planning and preparedness to respond to a terrorist attack, to include WMD usage.
- **Coverage for Off-Base Assets** - In planning the coverage of off-base assets and infrastructure selected for inclusion in the facility, installation, or activity AT program, include notifications to the appropriate first responders, including law enforcement offices, and the servicing FBI field office. This action enables integration of the off-base facility into their response and contingency planning and provides a potential source to assist the facility in its own preparations and response. As necessary, validate and monitor the scope and viability of the coverage. If the asset is a cleared contractor facility, provide for reporting to the servicing Defense Security Service (DSS) Industrial Security Field Office of information that indicates classified information under facility control is or could be at risk. Promptly notify the servicing DSS office of any security requirements that the installation or activity intends the cleared industrial facility to implement.

The Antiterrorism Officer (ATO) is normally assigned the task of writing the AT plan, while the responsibility for developing the plan rests with the organization's Commander. A Commander's involvement is essential for the creation of a sound plan. The ATO should leverage the capabilities of the organization's AT Working Group to assist with creating an AT plan.

Several resources and tools are available to personnel involved with developing an AT plan. Personnel should be familiar with:
- DoDI 2000.12 DoD AT Program
- DoDI 2000.16 DoD AT Standards
- DoD ATO Guide

**AT Plan Format**

When writing an AT plan, the ATO's biggest challenge is selecting a format that ensures that the organization will be able to understand the plan and execute it quickly and decisively when required.

AT Plan formats may vary throughout the different services and organizations, however, the recommended AT plan format is the standard five-paragraph format outlined in the Joint Publication 5-00.2, "Joint Task Force Planning Guidance and Procedures." The five-paragraph format is as follows:
- **Situation (S)**
- **Mission (M)**
- **Execution (E)**
- **Administration and Logistics (A)**
- **Command and Signal (C)**

**Note**: In addition to the five paragraphs, an AT plan also has Annexes.

**Situation**

The first paragraph of an AT plan is Situation, comprised of the following sections:
- **General** - Describes the political/military environment in sufficient detail for subordinate Commanders, staff, and units to understand their roles in the installation of AT operations.
• **Enemy forces** - Describes the general threat of terrorism to the installation including the intentions and capabilities, identification, composition, disposition, location, and estimated strengths of hostile forces. Also included is the general threat of terrorists using WMD against the installation.

• **Friendly forces** - Discusses the installation's AT posture and forces available, including the next higher headquarters and adjacent installations. Also included is information on any units not under installation command required to assist in AT planning and execution.

• **Attachments and detachments** - Identifies the attached or detached units such as reserve units, which are mustering and/or training at the installation.

• **Assumptions** - Identifies all critical assumptions unlikely to change during the implementation of the AT plan. Assumptions may range from natural disasters as part of the threat to the major political/social environment in the surrounding area.

• **Intelligence** - Identifies the person(s), staff, or units responsible for intelligence collection and dissemination.

**Mission**

The second paragraph of the AT plan is Mission. The Mission paragraph contains a clear, concise statement of the command's mission and the AT purpose or goal supporting the mission. The primary purpose of the AT plan is to safeguard personnel, property, and resources during normal operations. It is also designed to deter a terrorist threat, enhance security and AT awareness, and assign AT responsibilities for all installation personnel. In order to complete the Mission, the installation should meet the following four objectives:

- Deter terrorist incidents
- Employ countermeasures
- Mitigate the effects of a terrorist incident, and
- Recover from a terrorist incident

**Execution**

Execution is the third paragraph of the AT plan, and is comprised of the following sections:

- **Commander's Intent** - Describes command priorities, and how the Commander envisions the AT plan execution.

- **Concept of Operations** - Describes how the overall AT operation should progress. This section stresses the deterrence of terrorist incidents through preventive and response measures common to all combatant commands and Services. It should provide subordinates sufficient guidance to act if contact or communications with the installation chain of command is lost or disrupted.

  The installation's AT Concept of Operations should be phased in relation to:

  - **Pre-incident actions** - These occur during day-to-day operations. During this time, the installation should stress continuous AT planning and passive, defensive operations. AT planning and execution requires that staff elements work with a much greater degree of cohesiveness and unity of mission than required during normal operations

  - **Post-incident actions** - During post-incident planning, the installation should focus on its response and reconstitution responsibilities upon notification of a terrorist incident and the procedures for obtaining assistance if the incident exceeds the installation's capabilities. National level responders (e.g., Federal Emergency Management Agency (FEMA), Red Cross, and the Federal Bureau of Investigation (FBI)) may not be immediately accessible or available to respond to
an installation's needs. Therefore, each installation must plan for the worst-case scenario by planning its response based on available resources.

- **Tasks** - Lists the specific tasks for each subordinate unit or element listed in the Task Organization paragraph. The Commander should ensure that a specific individual/unit/element within the installation is responsible for each action identified in the AT plan.

- **Coordinating Instructions** - Identifies AT specific coordinating instructions, the Commander deems appropriate. This section also provides an outline illustrating the aspects of the installation's AT posture that require particular attention to guarantee the most effective and efficient implementation of the AT plan.

There are five basic Coordinating Instructions:

- AT planning and response elements - Identify the jurisdictional limits of the installation's Commander and key staff. This can be accomplished through either the Host Nation if OCONUS or the Local, State, and Federal U.S. authorities. These elements provide a synopsis of all agreements, as they relate to AT.

  **Note:** It is important to establish Memorandums of Agreement (MOAs) and Memorandums of Understanding (MOUs) with appropriate authorities, and to disseminate these documents accordingly.

- Procedures included in the instruction:
  - Alert notification procedures
  - Use of force/rules of engagement
  - Installation training and exercises
  - Incident response
  - Consequence management
  - High-risk personnel protection procedures

- Security posture responsibilities document the following responsibilities:
  - Operations security (OPSEC)
  - Access control
  - Barriers
  - Lighting
  - On-site security elements
  - Technology
  - Training

- Threat specific responsibilities document the following:
  - WMD
  - Information security

- Special installation areas document the following:
  - Airfield security
  - Port security
  - Buildings
  - Other

**Administration and Logistics**

The fourth paragraph of the AT plan is Administration and Logistics. This paragraph defines the requirements for supporting the AT plan, including enough information to make clear the basic concept for planned logistics support. This paragraph should address the following sections to ensure the staff conducts logistical planning for both pre-and post-incident measures:
Readiness & Concept of Combat Service Support - Lists service support instructions and arrangements supporting the AT plan. This section also describes the administrative and logistics requirements pertinent to the installations AT plan.

Material and services - Lists supply, maintenance, transportation, construction, and allocation of labor that apply to AT efforts prior to a terrorist attack.

Weapons and ammunition - Identifies the weapons and basic ammunition allowances required to support the AT augmented security forces.
  Note: Planners should identify the location, authority for issue, and basic level of issue.

Medical services - Lists plans, policies, and local/host nation agreements for AT treatment, hospitalization, and evacuation of personnel, both military and civilian.
  Note: Planners should include aerial medical evacuation support, directions to the nearest trauma center, the ability to set up a crisis center and WMD response capability, and the ability to support a mobile medical hospital.

Personnel - List procedures for strength reporting, replacements, and other procedures pertinent to base defense.

Civil affairs - Identifies the person, staff, or unit responsible for coordinating and interfacing with the local population to provide assistance for civilian needs in the event of casualties.

Updates to the AT installation plan - Identifies the appropriate person(s), staff, or unit responsible for developing a process for updating this plan and for distributing those updates.

Command and Signal

The fifth and final paragraph of the AT plan is Command and Signal.

- Command section defines command relationships to include command succession and the chain of command for AT issues.
- Signal section describes communication assets and procedures to support AT efforts. This paragraph identifies the primary and alternate locations of the command post and operations centers. The Installation Commander must ensure that key AT staff members understand the differences inherent in their installation's incident response command structure, with special consideration to the location of the installation (CONUS/OCONUS). Communications for AT contingency operations will be the normal base communications augmented by additional electronic communications equipment, and couriers, and will meet IAW (in accordance with) Operations Security (OPSEC) and Communications Security (COMSEC) requirements.

Annexes

AT plan Annexes provide amplifying instructions on specific aspects of the plan. Each Annex can be subdivided into Appendices, Tabs, and Enclosures as required. There are eighteen Annexes of an AT plan.

- Annex A - Task Organization - contains all of the organizations involved with installing an Antiterrorism defense. Also included in this section are the AT requirements of the Host Nation, U.S., and other civilian organizations contained within the installation. The Task Organization must include the following information:
  - Who is in charge?
  - Who is responsible for what?
  - Command and staff relationships
  - Various AT Working Groups, and
  - Requirements

- Annex B - Intelligence - provides descriptions of the agency(s) responsible for intelligence and specific instructions pertaining to the following assessments:
Antiterrorism Officer Level II  
Antiterrorism/Threat Awareness

- Local Threat Assessment
- Local WMD Assessment
- Local Criticality/Vulnerability Assessment
- Risk Assessment
- Pre-deployment AT Vulnerability Assessment

- **Annex C - Operations** - provides specific instructions for the various AT operations. This annex will include information on how the installation will implement force protection measures. This is the MOST important part of the plan; all other Annexes/Appendices support the implementation of this Annex.

- **Annex D - Logistics** - provides specific logistics on how to support AT operations.

- **Annex E - Fiscal** - provides specific fiscal instructions on how to support AT operations from pre-incident through post-incident.

- **Annex F - Tenant Commanders** - provides specific instructions on how tenant commands/agencies support AT operations.

- **Annex G - Air Operations** - provides specific air instructions on how to support AT operations.

- **Annex H - Legal** - provides the jurisdictional limits of the installation's Commander and key staff. Although the Department of Justice and FBI have primary law enforcement responsibility for terrorist incidents, in the U.S., the installation Commander is responsible for maintaining law and order on the installation. For OCONUS incidents, the installation Commander must notify the Host Nation and the geographic combatant Commander who will notify the Department of State.

- **Annex I - Public Affairs** - provides specific Public Affairs Office (PAO) instructions on how to support AT operations.

- **Annex J - Command Relationships** - provides specific guidance on command relationships and military/civilian interoperability issues during incident command and control.

- **Annex K - Communications** - provides specific communications instructions on how to support AT operations; be sure to include system/procedures for SECURE and NON-SECURE communications means.

- **Annex L - Health Services** - provides specific medical instructions on how to support AT operations.

- **Annex M - Safety** - provides specific safety instructions on how to support AT operations.

- **Annex N - AT Program Review, Training, and Exercises** - provides detailed information for each.

- **Annex O - Personnel Services** - provides administrative and personnel procedures required to support the plan (i.e., civilian overtime, and post-traumatic stress syndrome counseling).

- **Annex P - Reports** - provides all of the procedures for report submission and formatting.

- **Annex Q - References** - provides all supporting reference materials, publication, regulations, etc.

- **Annex R - Distribution** - provides the list of agencies to receive this plan and covers plan classification, handling, and declassification procedures.

**AT Plan Exercises**

Exercising the AT plan provides leaders, staff, and personnel realistic experiences in preparation for accomplishing wartime or special mission tasks, and plays an important role in the AT program. The exercise:

- Assists the organization/installation with maintaining operational readiness
- Provides the organization with a means to document and measure operational readiness
- Validates the identified plan's capabilities
• Confirms training adequacy
• Provides a way to assess and identify vulnerabilities and resources
• Demonstrates a commitment to continuous AT improvement
• Increases antiterrorism awareness, and
• Provides a way to identify and prioritize needed force protection resources

These are the three types of AT plan exercises:
• **Table-top** - Requires key leaders and staff officers of an organization or installation to attend a facilitator-led scenario driven discussion. They can be used to exercise either specific portions or the entire AT plan. Table-top exercises should be used when an AT plan is new, as refresher training, or to familiarize new leaders to the AT plan.
• **Drill** - Scenario driven events usually limited to specific organizations or functions in order to test, assess, and validate specific portions of an AT plan such as command post exercises, notification drills, first responder drills, and evacuation drills.
• **Full-scale** - Most complex type of AT exercise and will most likely involve an entire organization and installation. For many key organizations and tenant units, this exercise will be the major focus of training for days and weeks leading up to the event as units will activate portions or all parts of their AT plan. This exercise requires extensive planning and should be used to validate the AT plan and timelines, assess functional capabilities and skills, and test equipment.

**Knowledge Check**

Try answering the following questions.

1. Which of the following requirements must be integrated into a comprehensive AT plan?
   a. Terrorist Incident Response Measures
   b. Intelligence Assessment
   c. WMD Assessment
   d. AT FPCON Measures

2. The recommended AT plan format consists of which of the following paragraphs?
   a. Command and Signal
   b. Execution
   c. Intelligence
   d. Coordinating Instructions

3. Which part of the AT plan provides amplifying instructions on specific aspects of the plan?
   a. Situation
   b. Mission
   c. Annexes
   d. Execution

4. AT plan exercises are important because they:
   a. Demonstrate a commitment to continuous AT improvement
   b. Validate the identified AT plan's capabilities
   c. Verify the cost of a full-scale exercise
   d. Assist the organization or installation with maintaining operational readiness

5. Which of the following statements are correct?
   a. The ATO is responsible for writing the AT plan.
   b. The Commander is responsible for the development of the AT plan.
   c. The ATO is responsible for leveraging the capabilities of the organization's AT Working Group to assist with creating the AT plan.
   d. The Commander writes the AT plan.
6. Which AT plan exercise involves key leaders and staff officers of an organization to attend a facilitator-led scenario driven discussion?
   a. Full-scale
   b. Drill
   c. Table-top
   d. All of the above

Lesson Conclusion

In this lesson, you learned about the roles and responsibilities for creating an AT plan, the requirements and format of an AT plan, and how to test the AT plan.
Lesson 4: Antiterrorism Resource Requirements

Lesson Introduction

Antiterrorism resource requirements used for defensive measures compete against the costs necessary for electricity, water, fuel, and installation maintenance. Commanders must make difficult decisions in prioritizing and funding these requirements.

The lesson objectives are:
• Identify resource requirements
• State the categories for justifying and prioritizing resource requirements
• Apply knowledge of requirements to complete documentation for resources
• Identify funding sources for additional resources
• Define ATO resource responsibilities

Resource Requirements

Resource requirements must be clearly identified, documented, and prioritized before an installation can successfully compete and acquire necessary funding. It is essential for the Commander to ensure an AT plan is developed to adequately identify the resource requirements necessary to mitigate threat and vulnerabilities. The Commander must:
• Identify responsibilities for threat assessment, mission, execution, logistics, and command and control
• Document what, when, where, and how AT resources are needed
• Address and introduce as many tactics, techniques, and procedures, changes and measures as possible when writing baseline and higher Force Protection Condition and weapons of mass destruction plans
• Have consistent Random Antiterrorism Measures (RAM) with appropriate resources to ensure the plan is executable

The AT Plan must be based on the current threat and the critical assets that have been identified. The Vulnerability Assessment (VA) is critical to assess the organization’s current AT effectiveness with regard to: manpower, policy, procedures and plans, equipment, and training and exercises.

As you learned earlier in the course, there are three types of Vulnerability Assessments available to the installation Commander: Joint Staff Integrated Vulnerability Assessment (JSIVA), local vulnerability assessment, and service-level integrated vulnerability assessment.

During integrated vulnerability assessments, a higher headquarters assessment team will provide both procedural and resource recommendations to mitigate vulnerabilities and reduce risk. These recommendations, however, do not translate into a resource requirement; it is the Commander’s decision, with the assistance of the Antiterrorism Working Group, to determine how to address these recommendations, determine if the risk is acceptable, address the issues, and determine if additional resources are necessary.

Once asset, threat, vulnerability, and AT effectiveness information is gathered, the Commander and the AT Working Group must analyze the data to assess the likelihood of the threat and the nature and scope of potential harm to critical assets. Be sure to address available technology, the affordability of the asset, and supportability costs (life cycle costs) as well as the current effectiveness of existing resources. This analysis lays the foundation for risk management. Once this analysis is completed, the AT plan is exercised, lessons are learned, and the level of risk is identified. If it is determined that additional resources are required, the requirements are prioritized and documented.
Prioritizing Resources

Once requirements are identified, it is important to justify and prioritize them to ensure the most critical requirements are funded first and can effectively compete against other resources.

Resources should be given priority when they are required to mitigate a major or high-risk situation, or are necessary to adhere to the DoD or Service directives, standards, instructions, or regulations. To justify and prioritize resource requirements, the Commander must articulate all aspects of:

- **Threat** - Determined by using the DoD threat methodology (see Terrorism Lesson) to describe the type of threat to protect against.
- **Asset criticality** - Determined by describing the importance of the asset and the effect or ramifications of its loss.
- **Vulnerability** - Determined by assessing and describing construction standards, accessibility to the asset, and recognizability of the asset.
- **Current AT program** - Determined for a clear picture of current capabilities with regard to manpower, policy, procedures, plans, equipment, training, and exercises as designated in the AT plan.

Taking all four into consideration, the Commander must assess the risk and likelihood of an incident occurring and either accept the risk or mitigate the risk through changes in tactics, techniques, procedures or acquiring additional resources.

To assist in the prioritization of resources, the Commander, with the assistance of working groups, should place the resource requirements into three categories of importance: must fund, need to fund, and should fund.

Even though a requirement is identified as a must, need, or should fund asset, the requirement must be affordable, supportable, able to reduce risk, and provide a high/moderate impact on the AT program to achieve the objectives identified in the AT plan (deter, detect, defend, and respond). Once the requirements have been prioritized and categorized, an acquisition strategy needs to be researched, requirements submitted, and funding sources sought.

**Must Fund:** This category represents resources that are required to mitigate major or high risk situations. The criteria for a “must fund” asset includes:

- Threat to the asset is of high significance.
- The asset is a likely target, critical to the mission, and the threat is of a high impact that would require significant time to restore operations.
- The asset has significant vulnerabilities, weak structural protection and is recognizable and accessible.
- The assets are not available for baseline AT program or higher FPCON measures and there are no other mitigation capabilities.
- The Commander’s risk, which is major, indicates an unacceptable impact on mission readiness.

**Need to Fund:** This category represents resources that are in a medium risk category with medium vulnerabilities and moderate asset criticality. The criteria for a “need to fund” asset includes:

- Threat to the asset is high to moderate significance.
- The asset is a likely target and is moderately critical to the mission. The threat involves a large number of people and requires a moderate timeframe to restore operations.
- The asset has moderate vulnerabilities. It is accessible, lacks perimeter/access control, is recognizable, important and is a lucrative structure.
- The asset may be necessary to execute higher FPCON AT measures; however, short-term mitigation capability is available.
- The Commander's risk is considerable/moderate, which relates to a long-term impact on mission readiness.

**Should Fund:** This category represents lower risk resources with minimal vulnerabilities and lesser asset criticality. The criteria for a “should fund” asset includes:
- The asset relates to all threat levels.
- The asset is important to the mission. The threat involves many people, but would require a short time to restore operations and redundant capabilities exist.
- The asset has low vulnerability. It is less accessible with moderate protection, is less recognizable but is identified as vulnerable.
- Assets are available for FPCON baseline and one level higher; however, longer-term mitigation capability is available.
- The Commander’s risk is lower, which relates to short-term impact on mission readiness.

**Prioritization Matrix**

The matrix shown below can be used by installations to prioritize their projects across all categories. Projects with the lowest point value have the highest priority for funding consideration.

![Prioritization Matrix Example - Requirements Justification](image)

**NOTE:** A requirement does not need to be associated with only one category.

**Documenting Resource Requirements**

Documenting resource requirements is crucial in articulating and justifying need and effectively competing for the funding necessary to acquire the resource.

A formal DoD AT requirements documentation and prioritization methodology has been established by the Joint Staff and the Office of the Secretary of Defense and adopted by the Services. This methodology is used to document and prioritize requirements for the DoD Planning, Programming, Budgeting, and Execution Process (PPBE), the Combating Terrorism Readiness Initiatives Fund (CbTRIF), and the Combatant Commander Command and Control Initiatives Program (C2IP), which will be discussed later in this lesson.

The Mission Assurance Risk Management System (MARMS) will be the replacement for CVAMP. MARMS will:
- Integrate AT and DCIP databases with enhanced capabilities to meet risk management requirements
- Include Information Assurance, CBRNE, COOP and Installation Emergency Management
- Provide capability to analyze threat and hazard data
- Provide alerts and notifications, and
- Provide report capabilities and training information
When submitting requirements it is important to address four key points:

- What resource is needed?
- Why the resource is needed?
- How the resource fits into the AT plan.
- Impact if the resource is not funded.

Once the requirements are understood and approved, a realistic fiscal year budget and procurement strategy should be established.

**Funding Sources**

Prior to seeking programmatic solutions, which involves requesting additional funding from outside of the installation budget and current resources, such as through unified commands, to address requirements, the Commander must first look at maximizing non-programmatic solutions, which include training, procedures, tactics, techniques, and engagement strategies, to determine if the need exceeds an acceptable risk.

**Planning, Programming, and Budgeting System (PPBS)**

The Planning, Programming, and Budgeting System (PPBS) is an annual process that produces Defense Planning Guidance, Program Objective Memorandum for Military Departments and Defense Agencies and a budgeting process to produce the President's National Budget.

Management Initiative Decision 913, Implementation of a 2-Year Planning, Programming, Budgeting, and Execution process dated May 22, 2003, modified the PPBS cycle to increase the effectiveness of the programming and budgeting process and to add additional emphasis on execution.

In response, DoD converted the annual Program Objective Memorandum (POM)/Budget Estimate Submission (BES) cycle to a biennial cycle. The emphasis is now on even years, when the 2-year budgets are formulated, with "off years" focusing on budget execution and program performance. For off years, no POM/BES will be submitted, and only changes to the preceding year's POM/BES will be addressed.

**Combating Terrorism Readiness Initiatives Fund (CbTRIF)**

The second source of funding is through the Combating Terrorism Readiness Initiatives Fund (CbTRIF). The purpose of the CbTRIF is to finance emergent (executed twice a year) or emergency (executed as required) high-priority combating terrorism requirements. The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5261.01 establishes policy and procedures to facilitate execution of the fund and is managed by the Chairman of the Joint Chiefs of Staff.

The Mission Assurance Risk Management System (MARMS) is required for submission of all CbTRIF requests. The Joint Staff, Deputy Director for Antiterrorism/ Force Protection (J34) manages this program for the Chairman of the Joint Chiefs of Staff. The fund provides a means to react to unanticipated requirements from changes in terrorist threats, threat levels, force protection doctrine/standards, as well as unanticipated requirements identified as a result of vulnerability assessments, tactical operations and exercising AT plans. The fund is NOT intended to subsidize ongoing projects, supplement budget shortfalls, support routine activity that is normally a Service responsibility, or handle the majority of force protection resource requirements.
Combatant Commander Command and Control Initiatives Program (C2IP)
The Combatant Commander Command and Control Initiatives Program (C2IP) is for combatant command use only. C2IP enables combatant commander’s to implement timely, low-cost, near term improvements to their C2 systems to meet requirements that result from unforeseen situations. C2IP is NOT intended to subsidize on-going projects or circumvent the PPBS.

ATO Resource Responsibilities

The ATO becomes the expert within the organization for generating, prioritizing, and appropriately documenting AT requirements. The ATO is responsible for establishing and maintaining a formal documentation methodology documenting AT resource requirements with regard to threat, asset criticality, vulnerabilities, current AT program effectiveness, and Commander’s risk. Requirements must be continuously documented and ready for funding data calls for information.

Once the ATO has documented resource requirements, the information needs to be articulated and justified to the installation AT working groups, budget personnel, and the Commander. These personnel will decide to either accept the risk or fund the asset through:
- Existing organizational funds
- Alternative means (e.g. sharing resources, procedural changes), or
- The chain of command as an unfunded requirement

Knowledge Check

Try answering the following questions.

1. When assessing resource requirements, the Commander and AT Working Group should analyze gathered information and assess the:
   a. Threat and potential harm to critical assets
   b. Affordability of the required asset
   c. Current effectiveness of existing resources
   d. ATO’s capability to obtain the asset

2. Resources should be given priority when they are:
   a. Identified as part of the need to fund category
   b. Required to mitigate a major or high-risk situation
   c. Necessary to adhere to DoD or Service directives, standards, instructions, or regulations
   d. Justified as a resource needing additional funding

3. Non-programmatic solutions include:
   a. Offering additional training
   b. Funding through PPBE
   c. Refining engagement strategies
   d. Funding through CbTRIF

4. Which of the following statements are correct?
   a. Requirements are documented once a year for funding requests.
   b. The ATO determines either to accept a risk or request funding for an unfunded resource.
   c. The ATO is responsible for establishing and maintaining a formal documentation methodology documenting AT resource requirements.
   d. The ATO becomes the expert within the organization in generating, prioritizing, and appropriately documenting AT requirements.
5. Which funding category does a resource fall in if it is a likely target and critical to the mission?
   a. Need to fund
   b. Should fund
   c. Must fund

6. The CbTRIF fund:
   a. Funds emergency and emergent high-priority requirements in the year of execution
   b. Subsidizes ongoing projects
   c. Supplements budget shortfalls
   d. Is managed by J34 for the Chairman of the Joint Chiefs of Staff

Lesson Conclusion

In this lesson, you learned about identifying, prioritizing and documenting resource requirements. You also learned about available funding sources for additional resources.