Course Glossary

Course: Physical Security Planning and Implementation

Active Barriers: Barriers that require action by personnel or equipment to permit entry to authorized personnel or vehicles.

ATO: Antiterrorism Officer

ATWG: Antiterrorism Working Group

Biometrics: The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics.

Continuous Lighting: A series of fixed luminaries arranged to flood an area with overlapping cones of light continuously during the hours of darkness.

DCIP: Defense Critical Infrastructure Program

Emergency Lighting: Back-up lighting which is used during power failures or other emergencies when normal lighting systems are inoperative.

Espionage: The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation.

Force Protection Conditions (FPCONs): A Chairman of the Joint Chiefs of Staff-approved program standardizing the Military Services' identification of and recommended responses to terrorist threats against US personnel and facilities. This program facilitates inter-Service coordination. There are four FPCONs above normal: FPCON ALPHA, FPCON BRAVO, FPCON CHARLIE, and FPCON DELTA.

FPCON ALPHA: This condition applies when there is an increased general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of FPCON BRAVO measures. However, it may be necessary to implement certain measures from higher FPCONs resulting from intelligence received or as a deterrent. The measures in this FPCON must be capable of being maintained indefinitely.

FPCON BRAVO: This condition applies when an increased or more predictable threat of terrorist activity exists. Sustaining the measures in this FPCON for a prolonged period may affect operational capability and relations with local authorities.

FPCON CHARLIE: This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely. Prolonged implementation of measures in this FPCON may create hardship and affect the activities of the unit and its personnel.

FPCON DELTA: This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. Normally, this FPCON is declared as a localized condition. FPCON DELTA measures are not intended to be sustained for substantial periods. See also antiterrorism; force protection.

Hard Target: Potential targets that provide a physical and psychological deterrence to intruders through the employment of physical security measures.

ISSM: Information System Security Manager

Memorandum of Agreement: Cooperative agreement is a document written between parties to work together on a mutually agreed upon project or to achieve a shared objective. An MOA is a written understanding of the agreement, which may be legally binding but may just be a statement of cooperation between the parties. Sometimes an MOA is interchangeable with a Memorandum of Understanding (MOU). Check with your Component for specific guidance.

Memorandum of Understanding: A document between two or more parties, describing an agreement between those parties. It expresses a shared intention to pursue a common line of action. Unlike a contract, an MOU does not legally obligate the parties, but it is more formal than a gentleman's agreement. Sometimes an MOU is interchangeable with a Memorandum of Agreement (MOA).

METT-TC: Mission, enemy, terrain and weather, troops, time, and available civilian considerations

Moveable Lighting: Mobile lighting normally used to supplement continuous or stand-by lighting.

OCOKA: Observations and fields of fire, cover and concealment, obstacles, key terrain, and avenues of approach

OPSEC: Operations Security—A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. See also operations security indicators; operations security measures; operations security planning guidance; operations security vulnerability.

Passive Barriers: Barriers with no moving parts and that rely on their bulk or mass to deny entry into a specific area or location.

Risk Management Process: The process of identifying, assessing, and controlling, risks arising from operational factors and making decisions that balance risk cost with mission benefits.

Sabotage: An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war materiel, premises, or utilities, to include human and natural resources.

Soft Target: Potential targets that have little or no security measures making it easier to breech the security.

Standby Lighting: Manually or automatically activated lights that are illuminated when suspicious activity is detected or suspected by the security force, alarm system, or motion detector.

Terrorism: The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. See also antiterrorism; combating terrorism; counterterrorism; force protection condition; terrorist; terrorist group.

Terrorist Threat Levels: An intelligence threat assessment of the level of terrorist threat faced by US personnel and interests in a foreign country. The assessment is based on a continuous intelligence analysis of a minimum of five elements: terrorist group existence, capability, history, trends, and targeting. There are five threat levels: NEGLIGIBLE, LOW, MEDIUM, HIGH, and CRITICAL. Threat levels should not be confused with force protection conditions. Threat level assessments are provided to senior leaders to assist them in determining the appropriate local force protection condition. (Department of State also makes threat assessments, which may differ from those determined by Department of Defense.)

Threat: An indication, circumstance, or event with the potential to cause loss of or damage to an asset or capability

TWG: Threat Working Group

Vulnerability: The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished.