# Glossary

## Course: Physical Security Measures

**Antiterrorism**: Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

**Area Security**: Consolidating assets into one area, installation, or facility and increasing the security for that particular area.

**Biometrics**: Measurable physical characteristics or personal behavioral traits used to recognize the identity, or verify the claimed identity, of an individual.

**Capability**: Facilitating method to implement a course of action. (A capability may or may not be accompanied by an intention)

**CCTV**: Closed circuit television is a security system with a camera that captures an image, converts it to a video signal, and transmits it to a monitoring station.

**Controlled Area**: A controlled space extending upward and outward from a specified point. This area is typically designated by a commander or director, wherein sensitive information or operations occur and requires limitations of access.

**CONUS**: Continental United States

**Counterintelligence**: The act of keeping sensitive information from an enemy, deceiving that enemy, preventing subversion and sabotage, and collecting political and military information.

**Electronic Security Systems (ESS)**: That part of physical security concerned with the safeguarding of personnel and property by use of electronic systems. These systems include, but are not limited to, intrusion detection systems (IDS), automated entry control systems (AECS), and video assessment systems.

**Enclaving**: designating islands of high security within a sea of moderate security.

**Installations**: Real DoD properties including bases, stations, forts (including National Guard and Federal Reserve Centers), depots, arsenals, plants (both contractor and Government operated), hospitals, terminals, and other special mission facilities, as well as those used primarily for military purposes.

**Intrusion Detection System**: A security system that is designed to detect a change in the environment and transmit some type of alarm notification.

**Physical Security**: The security discipline concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

**Premise Control Unit (PCU)**: The centralized device that receives changes in the environmental state from the intrusion detection equipment and transmits an alarm or trouble condition to the monitoring station.

**Point Security**: Guarding a specific asset or resource using a dedicated guard.

**Restricted Area**: An area (land, sea or air) in which there are special restrictive measures employed to prevent or minimize incursions and/or interference, where special security measures are employed to prevent unauthorized entry. Restricted areas may be of different types depending on the nature and varying degree of importance of the security interest, or other matter contained therein. Restricted areas must be authorized by the installation/activity commander/director, properly posted, and shall employ physical security measures. Additionally, Controlled Areas may be established adjacent to Restricted Areas for verification and authentication of personnel.

**Risk**: A measure of consequence of peril, hazard, or loss, which is incurred from a capable aggressor or the environment (the presence of a threat and unmitigated vulnerability).

**Risk Management**: Process and resultant risk of systematically identifying, assessing, and controlling risks. Commanders/Directors are required to identify critical assets and their subsequent protection requirements, including future expenditures required for the protection requirements.

**Sabotage**: Destruction of an employer's property (as tools or materials) or the hindering of manufacturing by discontented workers; destructive or obstructive action carried on by a civilian or enemy agent to hinder a nation's war effort; an act or process tending to hamper or hurt.

**Security-in-Depth**: A determination by the senior agency official that a facility's security program consists of layered and complementary security controls sufficient to deter, detect, and document unauthorized entry and movement within the facility. Examples include the use of perimeter fences, employee and visitor access controls, use of an intrusion detection system, random guard patrols throughout the facility during non-working and working hours, and closed circuit video monitoring or other safeguards that mitigate the vulnerability of unalarmed storage areas and security storage cabinets during non-working hours.

**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

**Theft**: The unlawful taking and removing of property with intent to deprive the rightful owner of it

**Threat**: The perceived imminence of intended aggression by a capable entity to harm a nation, a government or its instrumentalities, such as intelligence, programs, operations, people, installations, or facilities.

**Vulnerability**: A situation or circumstance, which left unchanged, may result in the degradation, loss of life, or damage to mission-essential resources.