REFERENCE: COURSE GLOSSARY

Purpose: The purpose of this reference is to provide a glossary of important terms.

Key Term	Description
Access (Mod 10)	The ability to gain entrance to asset
Active sensor (Mod 13)	An electronic device that transmits energy and detects change in the received energy
Addendum (Mod 01)	An addendum contains resource material that supports the presentation or exercise. Examples include job aids or worksheets. Addendums are located in the Participant Guide.
Adversary (Mod 10)	An individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities, detrimental to a government or facility
Animation (Mod 01)	An animation is a moving graphic element on a PowerPoint slide and is designed to illustrate key course concepts.
Application whitelisting (Mod 07)	A proactive security technique where only a limited set of approved programs are allowed to run, while all other programs (including most malicious software) are blocked from running by default; enables only the administrators, not the users, to decide which programs are allowed to run
Area lighting (Mod 11)	Artificial illumination that exposes locations inside the perimeter that intruders must cross in order to reach their objectives
Assessment (Mod 12)	A necessary step in the detection process to ensure whatever caused the alarm can be identified
Asset (Mod 02)	Person, structure, facility, information, material, or process that has value
Asset analysis (Mod 06)	The complete description of the types of assets under each sector or category of critical infrastructure and the identification of undesirable consequences for each type
ATA (Mod 01)	Office of Antiterrorism Assistance (US State Department)
Balanced protection (Mod 13)	A characteristic of an effective physical protection system that ensures no matter how a terrorist intruder attempts to accomplish the attack goal, the intruder will encounter effective elements of the physical protection system
Binary explosive (Mod 09)	An explosive manufactured and packaged in two different containers with each container housing a different component. Neither component is classified as an explosive until mixed when it becomes a detonator-sensitive explosive

Key Term	Description
Bistatic microwave sensor (Mod 13)	An electronic device composed of two identical microwave antennas installed at opposite ends of the detection zone
Blast seat (Mod 09)	The source of an explosives detonation
Blast wave (Mod 09)	An area of pressure expanding supersonically outward from the blast seat
Bypassing (Mod 13)	The act of going around a sensor's detection zone
CBRN (Mod 09)	Chemical, biological, radiological, and nuclear
CCTV (Mod 14)	Closed-circuit television
CISR (Mod 01)	Critical Infrastructure Security and Resilience
Collaboration (Mod 15)	The process of working together to achieve shared goals
Command-activated method (Mod 09)	Bomber initiated IED by remote control or command detonation
Community awareness program (Mod 04)	An interactive program designed to provide citizens with the basic tools needed to recognize and help prevent terrorism and criminal activity within our communities
Community engagement (Mod 03)	The process of fostering cooperation between community members and local government by establishing dialogue, building rapport, and strengthening relationships to enhance public safety and order
Community Engagement and Human Rights Discussion (Mod 01)	A community engagement and human rights discussion is an opportunity to examine the benefits of promoting human rights in the conduct of the participants' daily job functions.
Community partnerships (Mod 04)	Law enforcement agencies and the community and organizations they serve working together for the purpose of developing solutions to problems and increasing trust in law enforcement
Container (Mod 09)	An item or vessel that commonly houses or conceals the complete IED or principle components of the IED
Contingency planning (Mod 12)	A method to develop well-documented procedures for identifying potential targets, responding to potential threats, interacting with external agencies, and determining the level of use-of-force security can use in various situations
Contraband detection (Mod 13)	Examining personnel, materials, and vehicles to detect unauthorized items using metal detectors, package searches, and explosive detectors
Countersurveillance (Mod 08)	A reactive and offensive security measure used to confirm whether hostile surveillance is occurring
Critical asset (Mod 06)	Any people, information, processes, and equipment that must be protected to prevent an undesired consequence from occurring

Key Term	Description
Critical incident (Mod 11)	Any natural or man-made event, civil disturbance, or any other occurrence of an unusual or severe nature that threatens to cause or causes the loss of life or injury to citizens or severe damage to property and requires extraordinary measures to protect lives, meet human needs, and achieve recovery
Critical incident management plan (Mod 11)	A standardized plan that outlines processes and procedures for coordination and control of responses to a terrorist event or natural disaster
Critical infrastructure (Mod 02, Mod 07)	Systems and assets, whether physical or virtual, so vital to the nation that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters
Critical infrastructure assessment (Mod 05)	A comprehensive evaluation of the critical infrastructure components of a given critical infrastructure
Critical infrastructure assets (Mod 10)	The resources (people, information, processes, and equipment) that support the operation of a critical infrastructure
Critical infrastructure categories (Mod 02)	The sixteen sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the nation that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health, or safety, or any combination thereof
Critical infrastructure components (Mod 02)	The physical conditions, facility operations, policies and procedures, regulatory requirements, and the safety and legal considerations of the identified asset
Cross-border infrastructure (Mod 07)	Any critical services such as banking or telecommunications that are located in another country or have a crucial dependency on information systems outside of a given country's jurisdiction
CT (Mod 01)	Bureau of Counterterrorism (US State Department)
Cyberattack (Mod 07)	An intrusion into electronic and digital information systems, by way of cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of the data or stealing controlled information
Cyberinfrastructure (Mod 07)	Electronic or digital information and communication systems and databases, and the information contained in these systems; organizational intranets, shared networks, and the Internet are all part of cyberinfrastructure

Key Term	Description
Cyberinterdependency (Mod 07)	The compatibility and commonality of computer operating systems, networks, and databases across many systems
Cybersecurity (Mod 02, Mod 07)	Preventing damage to, unauthorized use of, or exploitation of electronic information and communication systems and databases and the information contained therein to ensure confidentiality, integrity, and availability; and restoring electronic information and communications systems in the event of a terrorist attack or natural disaster
Cybersecurity engineer (Mod 07)	A personnel role in the information technology department that aids in cybersecurity by determining who requires access to which information; plans, coordinates, and implements information security programs; and helps protect against Internet threats that facilitate cybercrime
Cyberspace (Mod 07)	A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers
Cyberthreat (Mod 07)	Any circumstance or event with the potential to adversely affect an information system by way of unauthorized access, destruction, disclosure, modification of information, or denial of service
Data call (Mod 05)	To request information about the site prior to actually performing the site visit
Decay (Mod 09)	A shock front's very rapid drop in pressure as it travels away from the blast seat; objects in the path of the shock front can affect the rate of decay
Deceit (Mod 10)	An overt act of trying to misinform someone to gain access
Delay (Mod 12)	The process of slowing down intruders' progress by increasing the time it will take intruders to achieve their goal
Deployable barrier (Mod 13)	An obstacle that is only activated when there is an actual threat or attack
Deployment (Mod 12)	The actions of the security force from the time communication is received that an intruder is attacking until the security force is in position to interrupt the intruder's actions
Detection (Mod 12)	A process in which an alarm sensor activates due to an intruder attack, a nuisance alarm, or false alarm
Deterrent (Mod 12)	Delay prior to detection; no value added to physical protection system

Key Term	Description
Diversion of materials (Mod 10)	The unlawful movement or transfer of funds, information, or equipment
DS (Mod 01)	Bureau of Diplomatic Security (US State Department)
Entry control (Mod 12)	A way to allow only authorized personnel and materials to enter the facility; detects and prevents attempted entry of unauthorized personnel and material
Error rate (Mod 13)	The percentage that a specific entry control technique or process falsely rejects an authorized person or falsely accepts an unauthorized person
European Union (Mod 05)	A group or confederation of European countries that adheres to a standardized system of laws
Explosion (Mod 09)	An extremely rapid release of energy (gases) in the observed physical forms of light, heat, sound, and a shock wave
Explosives (Mod 09)	Substances that have the potential to release a very large amount of energy in a very short period of time
False acceptance rate (Mod 12)	A measure of effectiveness of entry control; the frequency at which false identities or credentials are allowed entry (3 out of every 1000 entries)
False alarm (Mod 12)	Any alarm where the cause of activation cannot be determined
False rejection rate (Mod 12)	A measure of effectiveness of entry control; the frequency at which access to authorized personnel is denied (1 out of every 1000 entries)
Feasibility (Mod 02)	Implementing security measures that are logical based on the situation and considering time, financial resources, personnel, and resources that it will take to implement
Firewall (Mod 07)	A network security system designed to provide protection against outside attackers by shielding your computer or network from malicious or unnecessary network traffic and preventing malicious software from accessing the network
Flow rate (Mod 13)	The measure of the time it takes for an authorized person or material to successfully pass an entry or exit point
Force (Mod 10)	An overt attempt to overcome a physical protection security system by violence
Fragmentation (Mod 09)	Occurs when the blast pressure effect of the explosion breaks the material that had been part of the bomb or of nearby objects into pieces
Fragments (Mod 09)	Pieces of a bomb or nearby objects that are carried outward by the blast wave

Key Term	Description
Gap analysis (Mod 02)	The process of identifying the difference (the gap) between existing security measures and the necessary future security measure(s)
Gap analysis process (Mod 15)	The steps that security managers use to compare the **actual** performance of an existing physical protection system with its **potential** performance
Hacker (Mod 07)	A person who seeks to gain unauthorized access to the computer data of another person or organization
Handbook (Mod 01)	A handbook contains resource material that supports the presentation. Examples include a threaded case study or other information that participants use in multiple modules.
Handout (Mod 01)	A handout supports the presentation and is distributed at a designated point in the course. Examples include knowledge surveys or exercise injects.
Hostile surveillance (Mod 02, Mod 08)	The discreet monitoring of a person, facility, or area with the intent of gathering information to formulate a plan that will enhance the likelihood of a successful terrorist operation or attack
Human rights (Mod 03)	Freedoms established by custom or international agreement that impose standards of conduct on all nations
IED (Mod 09)	Improvised explosive device
Improvised explosive device (IED) (Mod 02, Mod 09)	Any device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract
Incident command post (Mod 11)	The location from which the incident commander manages search and response activities
Incident pressure (Mod 09)	Exerted at right angles to the point of detonation as the blast wave expands
Information system (Mod 07)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information
Information system-related security risks (Mod 07)	Those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider the effect on the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the nation

Key Term	Description
Information technology (Mod 07)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by a law enforcement agency — this includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources
Initiator (Mod 09)	The IED component that activates (initiates) the detonation of the explosive device (main charge)
Insider threat (Mod 07)	An authorized user of a computer system who attacks the system after logging in, exceeds their computer privileges, or violates organizational security policy or laws; may be a dissatisfied employee or a contractor with system access
Interruption (Mod 12)	The successful arrival of the security force at an appropriate location and in sufficient numbers to confront the intruder(s)
Intrusion detection (Mod 07)	The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents
Intrusion detection and prevention (Mod 07)	The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents
Intrusion detection and prevention system (Mod 07)	Software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents
Intrusion detection system (Mod 07)	Software that automates the intrusion detection process; may or may not be detectible to the intruder
Intrusion prevention (Mod 07)	*See* intrusion detection and prevention
Intrusion prevention system (Mod 07)	*See* intrusion detection and prevention system
Kg (Mod 09)	kilogram
kHz (Mod 13)	Kilohertz
Large vehicle-borne improvised explosive device (VBIED) (Mod 09)	Use of a large vehicle as the container and delivery method for an IED

Key Term	Description
Limited scope performance testing (Mod 02)	A physical protection system is likely to have many components that would require large-scale performance testing, which may be unrealistic. Instead, a limited scope performance testing can be conducted on only specific elements of a physical protection system
Line-of-sight (Mod 09, Mod 13)	An expression used to describe a straight line or unobscured view between the source of an explosion and its target
LVBIED (Mod 09)	Large vehicle-borne improvised explosive device
Main charge (Mod 09)	The primary explosive substance of an improvised explosive device
Marginal (Mod 14)	The rating used in evaluating effectiveness of a physical protection system; means that the system only partially meets identified protection needs or provides questionable assurance that those protection needs will be met should they arise
Minimum consequences of component failure (Mod 13)	A characteristic of an effective physical protection system that provides contingency plans so that the system can continue to operate even after a component fails
Monostatic microwave sensor (Mod 13)	An electronic device composed of a single antenna that is used to both transmit and receive
Mps (Mod 09)	Miles per second
Network (Mod 07)	A group of electronic components that share information or interact with each other in order to perform a function
Neutralization (Mod 12)	The point at which intruders' actions are stopped and intruders are no longer able to fight against the security force
Nonmaster key (Mod 11)	Unlocks only the lock for which it was made; opposite of a master key that is a single key that unlocks multiple locks
Nuisance alarm (Mod 12)	Any alarm not caused by an intrusion
Passive sensor (Mod 13)	An electronic device that detects energy emitted by intruder
Perimeter barrier (Mod 11)	A natural boundary, freestanding fence or wall, or the outer walls or divisions of a building
Physical protection system (Mod 02)	An integration of people, policies and procedures, and equipment for the protection of assets or facilities against all threats
Policies and procedures (Mod 02)	Basic written guidelines to ensure standard operational physical protection system effectiveness
Policy (Mod 11)	General guidance regarding an organization's operational standards
Power source (Mod 09)	Creates electrical energy for an electrically initiated IED
PPS (Mod 02)	Physical protection system

Key Term	Description
Probability of detection (Mod 13)	The likelihood that an intrusion detection system senses and actual threat or attack
Probability of occurrence (Mod 06)	The likelihood that a terrorist will attack or an undesirable event will happen
Procedure (Mod 11)	A specific series of tasks, steps, and processes necessary to accomplish a particular goal; how the organization intends to carry out operating policies
Progressive collapse (Mod 09)	Occurs when the collapse of one structural element causes the failure of adjoining structural elements
Protected paths (Mod 12)	Routes and areas that have been secured for security force response
Protection (Mod 15)	The capabilities necessary to secure the homeland against acts of terrorism and human or natural disasters
Protection-in-depth (Mod 13)	A characteristic of an effective physical protection system that requires an intruder to avoid or defeat a number of protective devices in sequence to reach an objective or target
Reflected pressure (Mod 09)	Occurs when incident pressure is not parallel to the direction the wave is traveling as a result of making contact with a structure
Resilience (Mod 02)	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions such as deliberate attacks, accidents, or naturally occurring threats or incidents
Response (Mod 12)	The actions taken by the security force to prevent intruder success
RSO (Mod 01)	Regional security officer
Sabotage (Mod 10)	The deliberate and malicious destruction of property with the intent to cause harm to people, equipment, processes, and information with the intent to disrupt or stop operations of a facility
Satisfactory (Mod 14)	The rating used in evaluating effectiveness of a physical protection system; means that all elements of the physical protection system are working effectively to maintain the expected level of security
Secondary critical assets (Mod 05)	Secure areas that are accessible only after entrance through a primary access controlled entry
Secure asset (Mod 11)	A person, structure, facility, information, material, or process requiring a high level of protection

Key Term	Description
Security (Mod 02)	The implementation of a set of procedures and processes that when taken as a whole have the effect of altering the ratio of undesirable events to total event based on identified risks, threats, vulnerabilities, and probability of an undesirable occurrence
Security control center (Mod 05)	A room or building that serves as the primary command and communication hub for all security-related information and systems
Security countermeasures (Mod 02)	An action, measure, or device intended to reduce an identified risk
Security force (Mod 02)	A personnel-based security countermeasure
Security inspection and validation program directive (Mod 14)	A written order for implementing and conducting a security inspection and validation program on a regular basis
Security policy (Mod 11)	A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources
Seismic sensor (Mod 13)	A device that detects vibrations in the ground, most often used to detect the magnitude of earthquakes
Shock front (Mod 09)	The leading edge of a blast wave; made of compressed gasses
Shrapnel (Mod 09)	Materials such as nails, ball bearings, or fence staples included in the construction of a bomb to produce uniform fragments that will be carried outward by the blast wave that are intended to deliberately inflict additional personal and property damage
SIV (Mod 14)	Security inspection and validation
SME (Mod 14)	Subject matter expert
Spoofing (Mod 13)	The act of passing through a sensor's normal detection zone without triggering the alarm
Stealth (Mod 10)	An act of completing an adversarial task without being noticed, or going undetected
Subject matter expert (Mod 14)	Person with real expert knowledge about what it takes to do a particular job
Surveillance (Mod 08)	The monitoring of a person, facility, or area with the intent of gathering information, generally through discreet observation

Key Term	Description
Surveillance detection (Mod 02, Mod 08)	A defensive security operation used to determine whether a person or persons are conducting hostile surveillance; conducted temporarily or (for some critical infrastructures) permanently by an individual or full-time by a trained team to observe, recognize, and confirm suspicious activities
Surveillant (Mod 08)	A person conducting surveillance
Suspicious activity (Mod 04)	Any observed behavior that could indicate terrorism or terrorism-related crime
Switches (Mod 09)	IED component that is used to make, break, or change a connection between the power source, initiator, and main charge
TeachBack (Mod 01)	A TeachBack is a way to confirm that participants have learned by asking them to explain the content back to the facilitator. It is a test of how well facilitators explained a concept. This type of exercise provides another opportunity for participants to recall what they have been taught and practice their public speaking skills.
Terrorism (Mod 03)	Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents Title 22, Section 2656f(d) of the United States Code
Terrorists (Mod 10)	Individuals who unlawfully use force against persons or property to intimidate or coerce a government and its civil population to achieve a political or social objective
Theft (Mod 10)	The unlawful possession of property, equipment, information, materials, or other valuable products; may also refer to unlawful diversion of funds or information
Threaded exercise (Mod 05)	A scenario-based progressive learning activity that builds upon the learning objectives outlined in the modules in which the exercise occurs
Threat (Mod 06)	Natural or man-made occurrence, individual, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property
Threat analysis (Mod 06)	Product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, the environment, and/or property
Threat spectrum (Mod 06)	The range of potential threats to a critical infrastructure asset
Threat spectrum matrix (Mod 06)	A table that visually illustrates the relationships between consequence, level of consequence, and probability of occurrence

Key Term	Description
Throughput (Mod 12)	A measure of effectiveness of entry control; the number of authorized personnel allowed access per unit of time
Time-activated method (Mod 09)	Use of a switch that functions after a set time is reached
TNT (Mod 09)	Trinitrotoluene (explosive material)
Treaty (Mod 03)	A formal agreement between two or more states
Type I error (Mod 13)	The false rejection of an authorized person
Type II error (Mod 13)	The false acceptance of an unauthorized person
UDHR (Mod 03)	Universal Declaration of Human Rights
UN (Mod 03)	United Nations
Unsatisfactory (Mod 14)	The rating used in evaluating effectiveness of a physical protection system; means that the elements of the physical protection system are not functioning as designed and that the effectiveness has been reduced to the point of failure
US (Mod 01)	United States
VAM (Mod 02, Mod 05)	Vulnerability analysis methodology
VBIED (Mod 09)	Vehicle-borne improvised explosive device
Vehicle-borne improvised explosive device (VBIED) (Mod 09)	Use of a vehicle as the container and delivery method for an IED
Victim-activated method (Mod 09)	Use of a switch that activates by the actions of an unsuspecting individual
Vulnerability (Mod 02)	A physical feature or operational attribute that renders an entity open to exploitation or susceptible to given threat
Vulnerability analysis (Mod 02)	A product or process of identifying physical features or operational attributes that renders an entity, asset, system, network, or geographic area susceptible or exposed to threats
Vulnerability analysis methodology (Mod 02)	A systematic approach that security experts use to detect vulnerabilities and determine the level of effectiveness of a physical protection system
Vulnerability analysis team (Mod 05)	The people responsible for planning, conducting, and reporting on a vulnerability analysis; team members of may include a project manager, a security system technologist(s), and subject matter experts from the site