# Physical Security (V3.3 – Date Revised: 03.13.12)

## INTRODUCTION

**Participants should be made aware that the SPēD Diagnostic Tools are security reference resources to assist SPēD candidates gauge their individual level of expertise in the industrial, information, personnel, and physical security disciplines as well as general security topics. The questions within the SPēD Diagnostic Tools are different from those in the Security Fundamentals Professional Certification (SFPC) Assessment. The diagnostic is not meant to be a study guide.**

The Security Fundamentals Diagnostic Assessment:

(1) Models the types of questions used in the SFPC Assessment.

(2) Affords security professionals an opportunity to assess their understanding of security topic areas, i.e., General Security, Industrial Security, Information Security, Personnel Security, and Physical Security.

This document focuses on **Physical Security**. Diagnostic items are associated with seven Physical Security topic areas:



The correct answer choice is presented directly below each item.

If you have any questions/concerns regarding the items on the diagnostic, contact the SPēD Program Management Office at sped@dss.mil. You must provide a complete explanation and applicable DoD references for each item in question. We appreciate your comments and will address your concerns in a timely manner.

Good luck!

# Physical Security (V3.3 – Date Revised: 03.13.12)

## TOPIC # 1: FACILITY ACCESS CONTROL PROCEDURES

**1.** Designation of a restricted area is the responsibility of the Physical Security Director.

A. True
B. False

Answer: (False)- (*DoD 5200.8-R, DL1.12*)

**2.** A restricted area must be properly marked to inform personnel they are in its vicinity.

A. True
B. False

Answer: (True)- (*DoD 5200.8-R, DL1.12*)

**3.** All individuals with the appropriate personnel clearance level are allowed access to a designated restricted area.

A. True
B. False

Answer: (False)- (*DoD 5200.8-R, DL1.12*)

**4.** Controlled areas may be set up adjacent to designated restricted areas to facilitate the verification and authentication of personnel.

A. True
B. False

Answer: (True)- (*DoD 5200.8-R, DL1.12*)

**5.** Restricted areas employ physical security measures to prevent unauthorized entry and/or minimize incursions or interference.

A. True
B. False

Answer: (True)- (*DoD 5200.8-R, DL1.12*)

**6.** Restricted areas may be of different types depending on the nature and varying degree of importance of the security interest.

A. True
B. False

Answer: (True)- (*DoD 5200.8-R, DL1.12*)

**7.** Only the Installation Commander or the Activity Director can authorize a restricted area.

A. True
B. False

Answer: (True)- (*DoD 5200.8-R, DL1.12*)

**8.** Two security professionals – **Jo and Chris** – are discussing facility access control procedures.

**Jo says** that admittance to a restricted area is typically limited to personnel assigned to the area and persons who have been specifically authorized access to that area.

**Chris says** that visitors to a restricted area must be escorted by personnel assigned to the area or by persons who have been specifically authorized access to that area.

**Who is correct?**

A. Jo is correct.
B. Chris is correct.
C. Jo and Chris are both correct.
D. Jo and Chris are both incorrect.

Answer: (C)- (*DoD 5200.8-R, C3.3*)

**9.** This facility access control procedure includes procedures for searching packages, vehicles, and personnel.

A. Identification Systems and Methods
B. Methods of Control
C. Entry and Exit Inspection

Answer: (C)- (*DoD 5200.8-R, C3.3*)

**10.** The facility access control procedure employs various types of entry control devices including the use of the Common Access Card.

A. Identification Systems and Methods
B. Methods of Control
C. Entry and Exit Inspection

Answer: (A)- (*DoD 5200.8-R, C3.3*)

**11.** This facility access control procedure employs the use of physical security countermeasures including automated entry control systems, exchange badge systems, and security personnel conducting physical inspection of your credentials.

A. Identification Systems and Methods
B. Methods of Control
C. Entry and Exit Inspection

Answer: (A)- (*DoD 5200.8-R, C3.3*)

**12.** This facility access control procedure employs escorts and access control rosters to ensure accountability for all visitors to an area.

A. Identification Systems and Methods
B. Methods of Control
C. Entry and Exit Inspection

Answer: (B)- (*DoD 5200.8-R, C3.3*)

**13.** The two-person concept requiring two people to be present at all times while in a defined area is an example of this facility access control procedure.

A. Identification Systems and Methods
B. Methods of Control
C. Entry and Exit Inspection

Answer: (B)- (*DoD 5200.8-R, C3.3*)

**14.** The use of an x-ray machine or metal detector to determine whether or not a person is bringing unauthorized items into an area is an example of this facility access control.

A. Identification Systems and Methods
B. Methods of Control
C. Entry and Exit Inspection

Answer: (C)- (*DoD 5200.8-R, C3.3*)

**15.** This facility access control procedure focuses on the unauthorized removal of government assets from an area; thus, it serves not only as a deterrent, but also as a means for detecting contraband.

A. Identification Systems and Methods
B. Methods of Control
C. Entry and Exit Inspection

Answer: (C)- (*DoD 5200.8-R, C3.3*)

**16.** The Homeland Security Presidential Directive 12 (HSPD 12) aims to reduce the number of systems used in this facility access control procedures by mandating common system criteria.

A. Identification Systems and Methods
B. Methods of Control
C. Entry and Exit Inspection

Answer: (A)- (*DoD 5200.8-R, C3.3*)

**17.** The use of different badges for visitors in an example of this facility access control procedure.

A. Identification Systems and Methods
B. Methods of Control
C. Entry and Exit Inspection

Answer: (B)- (*DoD 5200.8-R, C3.3*)

**18.** Two security professionals – **Jo and Chris** – are discussing facility access control procedures.

**Jo says** that, within the Department of Defense, the Common Access Card fulfills the requirements of the common identification criteria mandated by HSPD 12.

**Chris says** that, depending on the area sensitivity, some Department of Defense facilities may still require credentials in addition to the Common Access Card as part of their facility access control procedure.

**Who is correct?**

A. Jo is correct.
B. Chris is correct.
C. Jo and Chris are both correct.
D. Jo and Chris are both incorrect.

Answer: (C)- (*DoD 5200.8-R, C3.3*)

**TOPIC # 2: LOCK AND KEY SYSTEMS**

**1.** Two security professionals – **Jo and Chris** – are discussing lock systems typically used within the Department of Defense (DoD)

**Jo says** that the two primary types of locks used within DoD are combination locks and key operated locks.

**Chris says** that the type of locking device selected for use depends on the environment and the type of assets that require protection.

**Who is correct?**

A. Jo is correct.
B. Chris is correct.
C. Jo and Chris are both correct.
D. Jo and Chris are both incorrect.

Answer: (C)

**2.** Mortise locks are considered low security locking devices recessed into a door or container and are typically found in general office areas.

A. True
B. False

Answer: (True)

**3.** The two types of combination locks approved for use to safeguard classified information are the ones that meet the Federal Specification FF-L-2740 which are the X-07, X-08, X-09, S&G 2740 and combination padlocks that meet FF-P-110J.

A. True
B. False

Answer: (True)- (*FF-L-2740-electromechanical locks; FF-L-2937, UL standard 768 Group 1-R-mechanical combination locks; FF-P-110J=changeable combination padlocks)*

**4.** Low security padlocks provide limited to minimal resistance to forced or surreptitious entry.

A. True
B. False

Answer: (True)- *(( DoD Lock Program) (CID) A-A-59486B and A-A-59487B. Low security padlocks are required to meet Commercial Item Descriptions (CID) A-A-59486B and A-A-59487B. These CID replace cancelled Military Specification MIL-P-17802 (Low Security Padlocks) and Commercial Item Description Padlock A-A-1927)*

**5.** Lock and key control procedures should include a key register and an authorized user list.

A. True
B. False

Answer: (True)- *(DoD 5100.76-M C2.5.5)*

**6.** Key control procedures are necessary because corrective measures associated with lost or uncontrolled keys can be costly and time consuming.

A. True
B. False

Answer: (True)- *(DoD 5100.76-M C2.5.5)*

**7.** Electromechanical combination locks used to secure classified information must meet FF-L-2740 specifications.

A. True
B. False

Answer: (True)- *(FF-L-2740)*

**TOPIC # 3: PHYSICAL SECURITY CONCEPTS**

**1.** Two security professionals – **Jo and Chris** – are discussing the Department of Defense's (DoD) Physical Security Program.

**Jo says** that the DoD Physical Security Program uses active and passive measures to detect, deter, delay, and/or deny unauthorized access to personnel, installations, equipment, facilities, activities, and operations.

**Chris says** that one purpose of the DoD Physical Security Program is to prevent damage to the theft of, and/or loss of the Department assets.

**Who is correct?**

A. Jo is correct.
B. Chris is correct.
C. Jo and Chris are both correct.
D. Jo and Chris are both incorrect.

Answer: (C)- *(DoD 5200.8-R, C2.1)*

**2.** Two security professionals – **Jo and Chris** – are discussing the Department of Defense (DoD) Physical Security Program.

**Jo says** that physical security uses active and passive measures to safeguard personnel, installations, equipment, facilities, activities, and operations against espionage, sabotage, terrorism, damage, and criminal activity.

**Chris says** that prevention and protection are the primary purposes of a physical security program.

**Who is correct?**

A. Jo is correct.
B. Chris is correct.
C. Jo and Chris are both correct.
D. Jo and Chris are both incorrect.

Answer: (C)- *(DoD 5200.8-R, C2.1)*

**3.** To achieve security-in-depth, a security program needs to employ and deploy layers of complementary security controls to deter, detect, delay, assess, respond, and document unauthorized movement within the facility.

A. True
B. False

Answer: (True)- (*DoD 5200.8-R, DL1.17)*

**4.** A security program determined to have security-in-depth employs an integrated protective system of active and passive security controls.

A. True
B. False

Answer: (True)- *(DoD 5200.8-R, DL1.17)*

**5.** Security-in-depth is a security concept that calls for the systematic use of physical security measures in levels or steps to create different layers of protection.

A. True
B. False

Answer: (True)- *(DoD 5200.8-R, DL1.17)*

**6.** Because different assets may require different levels of protection, the security-in-depth concept calls for the use of different types of security controls to ensure that each asset has the same level of protection.

A. True
B. False

Answer: (False)- *(DoD 5200.8-R, DL1.17)*

**7.** This entity manages, implements, and directs the installation of a facility's physical security program.

A. Anti-Terrorism Working Group (ATWG)
B. Anti-Terrorism Officer
C. CI Support Personnel
D. Force Protection Working Group (FPWG)
E. Information Systems Security Managers (ISSM)
F. Installation Commander/Facility Director
G. Law Enforcement Officials
H. Legal Officers
I. Operations Security Officer
J. Physical Security Officer/Provost Marshal
K. Threat Working Group (TWG)

Answer: (J)- *(DoD 5200.8-R, C2.2)*

**8.** This entity has overall responsibility for the safety and protection of the people and property in an installation or a facility.

A. Anti-Terrorism Working Group (ATWG)
B. Anti-Terrorism Officer
C. CI Support Personnel
D. Force Protection Working Group (FPWG)
E. Information Systems Security Managers (ISSM)
F. Installation Commander/Facility Director
G. Law Enforcement Officials
H. Legal Officers
I. Operations Security Officer
J. Physical Security Officer/Provost Marshal
K. Threat Working Group (TWG)

Answer: (F)- *(DoD 5200.8-R, C2.2)*

**9.** This entity is responsible for assessing physical security requirements and for conducting criticality, vulnerability, and risk assessments.

A. Anti-Terrorism Working Group (ATWG)
B. Anti-Terrorism Officer
C. CI Support Personnel
D. Force Protection Working Group (FPWG)
E. Information Systems Security Managers (ISSM)
F. Installation Commander/Facility Director
G. Law Enforcement Officials
H. Legal Officers
I. Operations Security Officer
J. Physical Security Officer/Provost Marshal
K. Threat Working Group (TWG)

Answer: (B)- *(DoD 5200.8-R, C2.2)*

**10.** This entity is responsible for ensuring the proper and legal incorporation of security considerations.

A. Anti-Terrorism Working Group (ATWG)
B. Anti-Terrorism Officer
C. CI Support Personnel
D. Force Protection Working Group (FPWG)
E. Information Systems Security Managers (ISSM)
F. Installation Commander/Facility Director
G. Law Enforcement Officials
H. Legal Officers
I. Operations Security Officer
J. Physical Security Officer/Provost Marshal
K. Threat Working Group (TWG)

Answer: (H)- *(DoD 5200.8-R, C2.2)*

**11.** This entity is responsible for coordinating physical security measures to protect information systems.

A. Anti-Terrorism Working Group (ATWG)
B. Anti-Terrorism Officer
C. CI Support Personnel
D. Force Protection Working Group (FPWG)
E. Information Systems Security Managers (ISSM)
F. Installation Commander/Facility Director
G. Law Enforcement Officials
H. Legal Officers
I. Operations Security Officer
J. Physical Security Officer/Provost Marshal
K. Threat Working Group (TWG)

Answer: (E)- *(DoD 5200.8-R, C2.2)*

**12.** This entity supports the physical security mission by managing the installation's use of defensive measures to reduce the vulnerability of individuals and property from terrorist attacks.

A. Anti-Terrorism Working Group (ATWG)
B. Anti-Terrorism Officer
C. CI Support Personnel
D. Force Protection Working Group (FPWG)
E. Information Systems Security Managers (ISSM)
F. Installation Commander/Facility Director
G. Law Enforcement Officials
H. Legal Officers
I. Operations Security Officer
J. Physical Security Officer/Provost Marshal
K. Threat Working Group (TWG)

Answer: (B)- *(DoD 5200.8-R, C2.2)*

**13.** This entity supports the physical security mission by providing information on our adversaries' intentions and capabilities.

A. Anti-Terrorism Working Group (ATWG)
B. Anti-Terrorism Officer
C. CI Support Personnel
D. Force Protection Working Group (FPWG)
E. Information Systems Security Managers (ISSM)
F. Installation Commander/Facility Director
G. Law Enforcement Officials
H. Legal Officers
I. Operations Security Officer
J. Physical Security Officer/Provost Marshal
K. Threat Working Group (TWG)

Answer: (C)- (*DoD 5200.8-R, C2.2)*

**14.** This entity supports the physical security mission by facilitating the identification of critical information.

A. Anti-Terrorism Working Group (ATWG)
B. Anti-Terrorism Officer
C. CI Support Personnel
D. Force Protection Working Group (FPWG)
E. Information Systems Security Managers (ISSM)
F. Installation Commander/Facility Director
G. Law Enforcement Officials
H. Legal Officers
I. Operations Security Officer
J. Physical Security Officer/Provost Marshal
K. Threat Working Group (TWG)

Answer: (I)- *(DoD 5200.8-R, C2.2)*

**15.** Two Security Professionals – **Jo and Chris** – are discussing physical security threats.

**Jo says** that natural disasters are considered a physical security threat because they have the potential to damage DoD resources or interrupt activities or operations.

**Chris says** that, although natural disasters have the potential to damage DoD resources or interrupt activities or operations, they are not considered a physical security threat because they are natural occurring phenomena.

**Who is correct?**

A. Jo is correct.
B. Chris is correct.
C. Jo and Chris are both correct.
D. Jo and Chris are both incorrect.

Answer: (B)- *(DoDM 5200.01-V3, Enclosure 2 par 10)*

**16.** Which of the following is an adversary who uses the threat of violence to instill fear and intimidate governments to fulfill goals that are generally political, religious, or ideological?

A. Criminal
B. Foreign Intelligence Agents
C. Insider
D. Terrorists

Answer: (D)- *(DoD O-2000.12-H C1.4.1.32)*

**17.** Which of the following is an adversary that actively engages in intelligence activities against the U.S. in the interest of another country?

A. Criminal
B. Foreign Intelligence Security Service
C. Insider
D. Terrorists

Answer: (B)- *(DoD 5200.8-R C2.1.2.1 Joint Publication 1-02)*

**18.** This concept refers to an indication, circumstance, or event with the potential to cause loss of or damage to an asset.

A. Criticality
B. Threat
C. Vulnerability

Answer: (B)- (*DoD 5200.8-R DL 1.21)*

**19.** This concept refers to a situation or circumstance, which if left unchanged, may result in damage to mission-essential resources.

A. Criticality
B. Threat
C. Vulnerability

Answer: (C)- (*DoD 5200.8-R DL 1.21)*

**20.** This concept refers to weaknesses that can be exploited by an adversary to gain unauthorized access to or information from an asset.

A. Criticality
B. Threat
C. Vulnerability

Answer: (C)- *(DoD O-2000.12-H C1.4.1.35.4)*

**21.** This concept refers to the perceived imminence of intended aggression by a capable entity to harm a government's programs, operations, people, installations, or facilities.

A. Criticality
B. Threat
C. Vulnerability

Answer: (B)- (*DoD 5200.8-R DL1.18)*

**22.** This concept is based on both an asset's importance to national security, and the effect of its partial or complete loss.

A. Criticality
B. Threat
C. Vulnerability

Answer: (A)- (*DoD O-2000.12-H C6.2)*

**23.** Two Security Professionals – **Jo and Chris** – are discussing the physical security principles of point and area security.

**Jo says** that area security maximizes the effectiveness of response forces by focusing security efforts on a specific asset or resource.

**Chris says** that only point security allows a security professional to effectively protect assets from damage, loss, and theft.

**Who is correct?**

A. Jo is correct.
B. Chris is correct.
C. Jo and Chris are both correct.
D. Jo and Chris are both incorrect.

Answer: (D)- *(DoD 5200.8-R DL1.17 "Security –in-Depth)*

**24.** Two security professionals – **Jo and Chris** – are discussing the physical security principles of point and area security.

**Jo says** that security professionals employ both point and area security to protect assets from damage, loss, and theft.

**Chris says** that security professionals employ both point and area security in an integrated manner to protect national security.

**Who is correct?**

A. Jo is correct.
B. Chris is correct.
C. Jo and Chris are both correct.
D. Jo and Chris are both incorrect.

Answer: (C)- *(DoD 5200.8-R DL1.17 "Security –in-Depth)*

**25.** Two security professionals – **Jo and Chris** – are discussing threat levels and Force Protection Conditions (FPCON).

**Jo says** that the FPCON level set by authorized personnel dictates the security measures an installation enacts to prevent or mitigate hostile actions against its personnel, resources, facilities, and critical information.

**Chris says** that senior leaders use threat levels to assist them in determining the appropriate FPCON level.

**Who is correct?**

A. Jo is correct.
B. Chris is correct.
C. Jo and Chris are both correct.
D. Jo and Chris are both incorrect.

Answer: (C)- *(DoD 0-2000.12-H)*

**26.** Which of the following threat levels suggest that there are terrorists present but there are no indications of anti-U.S. activity?

A. Low
B. Moderate
C. Significant
D. High

Answer: (B)- *(DoD 0-2000.12-H, C10.2.3)*

**27.** Which of the following FPCON levels indicates the existence of an increased threat of terrorist activity?

A. FPCON ALPHA
B. FPCON BRAVO
C. FPCON CHARLIE
D. FPCON DELTA

Answer: (B) *–( DoD 0-2000.12-H, Para C10.2.4.)*

**28.** Two security professionals – **Jo and Chris** – are discussing Crime Prevention Programs.

**Jo says** that the Department of Defense (DoD) considers criminals a threat because they have the potential to cause the loss of or damage to DoD assets or operations.

**Chris says** that crime prevention is a DoD Physical Security Program goal.

**Who is correct?**

A. Jo is correct.
B. Chris is correct.
C. Jo and Chris are both correct.
D. Jo and Chris are both incorrect.

Answer: (C)- *(DoD 5200.8-R C2.1.2.4)*

**TOPIC # 4: PROTECTIVE BARRIERS**

**1.** The first layer of an integrated physical security system typically uses protective barriers to protect a facility's perimeter.

A. True
B. False

Answer: (True)- *(DoD 5200.8-R, C2.1)*

**2.** The perimeter of an installation or facility is the outermost area of security responsibility for physical security practitioners.

A. True
B. False

Answer: (True)- *(DoD 5200.8-R, C2.1)*

**3.** Protective barriers such as poured concrete or hardened steel barriers are used for establishing perimeter boundaries.

A. True
B. False

Answer: (True)- *(DoD 5200.8-R, C2.1)*

**4.** Protective barriers deter individuals from attempting unlawful or unauthorized entry.

A. True
B. False

Answer: (True)- *(DoD 5200.8-R, C2.1)*

**5.** Protective barriers such as fencing can also be used as platforms for sensors and lighting.

A. True
B. False

Answer: (True)- *(DoD 5200.8-R, C2.1)*

**6.** Two security professionals – **Jo and Chris** – are discussing protective barriers.

**Jo says** that protective barriers can be used to enforce facility access control.

**Chris says** that protective barriers can be used to harden a facility.

**Who is correct?**

A. Jo is correct.
B. Chris is correct.
C. Jo and Chris are both correct.
D. Jo and Chris are both incorrect.

Answer: (C)- *(DoD 5200.8-R, C2.1)*

**TOPIC # 5: SECURE ROOMS, CONTAINERS, AND VAULTS**

**1.** Secure rooms and vaults are areas designated and authorized for the open storage of classified information.

A. True
B. False

Answer: (True)- *(DoDM 5200.01-V3 Enclosure 3)*

**2.** Vaults are different from secure rooms in that vaults typically meet SCIF construction requirements.

A. True
B. False

Answer: (False)- *(DoDM 5200.01-V3 Enclosure 3)*

**3.** Vaults have reinforced concrete on walls, ceilings, and floors, and have a hardened steel door.

A. True
B. False

Answer: (True)- (*DoDM 5200.01-V3 Enclosure 3)*

**4.** SCIFs are designed to store sensitive compartmented information – information that requires enhanced protection exceeding what is normally required for information at the same level of classification.

A. True
B. False

Answer: (True) – (*DOD 5105-21-M-1, ICD 705 (DNI))*

**5.** Secure rooms and vaults must be constructed to meet GSA-approved standards.

A. True
B. False

Answer: (False)- *(DoDM 5200.01-V3 Enclosure 3)*

**6.** Vaults and SCIFs must be constructed based on standards set in ICS 705.

A. True
B. False

Answer: (False)- (*DOD 5105-21-M-1; ICS 705 (DNI))*

**7.** GSA approves security containers used to store classified information.

A. True
B. False

Answer: (True)- *(DoDM 5200.01-V3 Enclosure 3)*

**8.** Secure rooms are usually built to commercial standards and provide a similar level of protection as a vault.

A. True
B. False

Answer: (False)- *(DoDM 5200.01-V3 Enclosure 3)*

**TOPIC # 6: SECURITY SYSTEMS DEVICES**

**1.** Two security professionals – **Jo and Chris** – are discussing access control systems.

**Jo says** that the choice of which access control system to use, manual or automated, should be determined by an analysis of the criticality, vulnerability, and the threat.

**Chris says** that access control is one of the inner layers in a security-in-depth approach to physical security.

**Who is correct?**

A. Jo is correct.
B. Chris is correct.
C. Jo and Chris are both correct.
D. Jo and Chris are both incorrect.

Answer: (C)- *(DoDM 5200.01-V3 Enclosure 3)*

**2.** Access control systems are implemented to prevent unauthorized personnel from entering a designated area.

A. True
B. False

Answer: (True)- (*DoDM 5200.01-V3 Enclosure 3)*

**3.** An example of a manual access control system is a stand-alone system that requires the user to know a three or four-digit number to gain access to the designated area.

A. True
B. False

Answer: (True)- (*DoDM 5200.01-V3 Enclosure 3)*

**4.** An example of a manual system that uses automated electronics is the Common Access Card that allows users to authenticate signatures, securely log onto computer systems, and gain access into designated areas.

A. True
B. False

Answer: (True)- *(DoDM 5200.01-V3 Enclosure 3)*

**5.** Biometric access control systems use individually unique characteristics such as fingerprints and voice to authenticate that an individual is authorized to gain access onto a designated area.

A. True
B. False

Answer: (True)- *(DoDM 5200.01-V3 Enclosure 3)*

**6.** Two security professionals – **Jo and Chris** – are discussing intrusion detection systems (IDS).

**Jo says** that an IDS uses sensors, control units, transmission line, and monitor units to detect a change in the environment.

**Chris says** that the two types of IDS are active and passive.

**Who is correct?**

A. Jo is correct.
B. Chris is correct.
C. Jo and Chris are both correct.
D. Jo and Chris are both incorrect.

Answer: (A)- *(DoDM 5200.01-V3 Enclosure 3)*

**7.** Two security professionals – **Jo and Chris** – are discussing intrusion detection systems (IDS).

**Jo says** that IDS can be used for area security.

**Chris says** that IDS can be used for point security.

**Who is correct?**

A. Jo is correct.
B. Chris is correct.
C. Jo and Chris are both correct.
D. Jo and Chris are both incorrect.

Answer: (C)- *(DoDM 5200.01-V3 Enclosure 3 5200.8-R C2.1.4.5 Based on a methodology)*

**8.** CCTV is considered cost effective because it allows security personnel to monitor multiple areas simultaneously.

A. True
B. False

Answer: (True)- *(DoD 5200.8-R C2.1.4.6 Based on a methodology)*

**9.** CCTV systems consist of sensors, control units, transmission lines, and monitor units.

A. True
B. False

Answer: (False)- *(DoDM 5200.01-V3 Enclosure 3)*

**10.** CCTV systems are used to prevent, deter, and detect pilferage.

A. True
B. False

Answer: (True)- *(DoD 5200.8-R C2.3)*

**11.** CCTV systems allow security personnel to safely assess and determine the size and intention of an unauthorized intrusion.

A. True
B. False

Answer: (True)- *(DoD 5200.8-R C2.3)*

**12.** CCTV systems provide security personnel the capability to detect, identify, track, assess, record, and coordinate response to unauthorized intrusions.

A. True
B. False

Answer: (True)- *(DoD 5200.8-R C2.3)*

**13.** Two security professionals – **Jo and Chris** – are discussing screening equipment.

**Jo says** that screening equipment is used in facility access control procedures.

**Chris says** that the use of screening equipment includes the use of two-way radios as a way for response forces to communicate with their respective control centers.

**Who is correct?**

A. Jo is correct.
B. Chris is correct.
C. Jo and Chris are both correct.
D. Jo and Chris are both incorrect.

Answer: (A)- *(DoD 5200.8-R C2.3.2.6.)*

**TOPIC # 7: SITE LIGHTING**

**1.** Site lighting enables guard force personnel to observe activities inside and around an installation.

A. True
B. False

Answer: (True)- (*MIL-HDBK-1013/1A 4.7.2)*

**2.** Site lighting discourages or deters attempts of unauthorized entry.

A. True
B. False

Answer: (True)- *(MIL-HDBK-1013/1A 4.7.2)*

**3.** Site lighting plays a large part in physical security, but its use should supplement other protective measures such as fixed security posts or patrols, fences, and alarms.

A. True
B. False

Answer: (True)- *(MIL-HDBK-1013/1A 4.7.2)*

**4.** Use of standby lighting is reserved for when regular lighting is not available.

A. True
B. False

Answer: (False)- *(MIL-HDBK-1013/1A 4.7.2)*

**5.** Use of emergency lighting is reserved for situations when additional lighting is necessary.

A. True
B. False

Answer: (False)- *(MIL-HDBK-1013/1A 4.7.2)*

**6.** Continuous lighting consists of a series of fixed lights arranged to continuously flood an area with overlapping cones of light.

A. True
B. False

Answer: (True)- *(MIL-HDBK-1013/1A 4.7.3.1)*