HANDOUT 1.1: PRE-COURSE KNOWLEDGE SURVEY

Select the best response to each question by drawing a circle around the letter corresponding to the response.

1. An assessment of a given critical infrastructure consists of _____.
   a. An appraisal of daily reports
   b. The efficiency of the personnel at the facility
   c. The evaluation of functional components
   d. The frequency of equipment maintenance

2. When an adversary is trying to penetrate or attack a critical infrastructure, the first two functions of a physical protection system include detection and delay. What is the third function of a physical protection system?
   a. Threat analysis
   b. Response
   c. Security inspection
   d. After-actions reporting

3. Which of the following are examples of critical assets?
   a. People, information
   b. Equipment, competitors
   c. Processes, currency
   d. Data, stocks

4. During a critical infrastructure assessment, a "data call" refers to:
   a. Scheduling a visit to the site
   b. Conducting a visit to the site
   c. Analyzing the information gathered during the site visit
   d. Requesting information about the site prior to the site visit

5. When law enforcement agencies and the community and organizations they serve work together for the purpose of developing solutions to problems and increasing trust in law enforcement, it is known as community _____.
   a. Alliance
   b. Cooperation
   c. Affiliation
   d. Partnership

6. Identifying all _____ is necessary before conducting an asset analysis.
   a. Hostile surveillants
   b. Critical assets
   c. Potential threats
   d. Undesirable consequences

7. Since it is not possible or practical to protect all critical infrastructure assets, you must:
   a. Ensure continuity of services by protecting government targets before civilian targets
   b. Provide protection for hard targets first, then soft targets second
   c. Protect your facilities before information and equipment
   d. Prioritize protection for assets according to their importance

8. Which of the following is any circumstance or event with the potential to adversely affect an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service?
   a. Cyberinfrastructure
   b. Cyberinterdependency
   c. Cyberthreat
   d. Cybersecurity

9. Robustness, resourcefulness, and rapid recovery are the three elements of _____ in your cybersecurity policies and procedures.
   a. Critical asset planning
   b. Resilience planning
   c. Physical protection system
   d. Gap analysis

10. As terrorist organizations prepare to launch an attack against a critical infrastructure site, _____ can be the weak link in their preparation process.
   a. Scope
   b. Security system tests
   c. Surveillance
   d. Acquisition of supplies

11. A person is observed on repeated occasions taking several quick photos of a critical infrastructure with a cell phone from several locations. This is an example of _____ that can indicate hostile surveillance.
   a. Normal behavior
   b. Unusual activities
   c. Surveillance detection
   d. Reporting actions

12. Which type of improvised explosive device currently poses the most destructive threat to a critical infrastructure?
   a. Pipe bomb
   b. Grenade
   c. Large vehicle bomb
   d. Letter bomb

13. Which of the following is the most effective security measure against a vehicle-borne improvised explosive device?
    a. Distance
    b. Reinforced structures
    c. Early detection
    d. Evacuation

14. The overall purpose of a threat analysis statement is to:
    a. Collect historical data about insiders who posed threats to the facility in the past
    b. Gather intelligence information on one or more threats
    c. Evaluate the security technology for a specific facility
    d. Determine if there are existing policies and procedures for a specific facility

15. The purpose of written procedures pertaining to critical infrastructure security is to:
    a. Replace the need for direct supervision by management
    b. Explain what the organization does operationally
    c. Explain the organization's position regarding security plans
    d. Provide consistent security force response

16. A process in which an alarm sensor activates due to an intrusion, a nuisance alarm, or false alarm is called:
    a. Assessment
    b. Delay
    c. Security force response
    d. Detection

17. The four primary elements that contribute to the effectiveness of a security force include: selection of security force members, initial and continuous training, deployment of adequate equipment, and _____.
    a. Extensive bomb crisis management experience
    b. Thorough knowledge of blast effects of explosives
    c. Appropriate supervision
    d. Specific training on the most current security technology

18. A passive sensor is typically one that:
    a. Is normally attached to the wall
    b. Detects some type of energy emitted by the intruder
    c. Is visible and therefore easy to defeat
    d. Transmits energy and detects a change in received energy

19. During _____ of the security inspection and validation program, you identify assets associated with the critical infrastructure.
    a. Phase 1: Inspection planning
    b. Phase 2: Conducting the inspection
    c. Phase 3: Asset evaluation
    d. Phase 4: Close-out

20. Which step of the gap analysis process determines what areas (risks) do not meet the pre-established performance standards or expectations?
    a. Step 1: Determine requirements
    b. Step 2: Assess existing performance levels
    c. Step 3: Identify gaps
    d. Step 4: Define risk management plan