Scenario 1

Cast

Rick: a cleared engineer
Manuel: a cleared senior engineer
Terry: a foreign national co-worker of Rick's
Jack: a newly hired cleared engineer
Unnamed: security manager

Brief Description of the Scenario

In Scenario 1, we meet Rick. Rick, a cleared engineer, is requesting classified information from a Security Manager for a research assignment he is currently working. In the beginning of the scenario, we learn whether the Security Manager has made the correct decision on whether Rick had the necessary requirements to gain access to the information. The next part of the scenario refers to the following day, when Rick gives the same classified information to a foreign national co-worker, named Terry, who has Limited Access Authority. The last section describes the following week, when another engineer gives Rick access to a different piece of classified information. Here, candidate questions focus on how they would react if the classified information was under special classification requirements (i.e., SCI, Foreign Government Information (FGI), and NATO).

This scenario aligns to the following security competencies:

INFORMATION SECURITY
Applies knowledge of policies, procedures, and requirements established under appropriate authorities to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security.

INCIDENT RESPONSE
Responds to crisis or urgent situations including accidents; man-made, biological, chemical, radiological, or natural disasters; and other incidents that could result in harm to people, property, or the environment. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life and preservation of property.

CLASSIFICATION MANAGEMENT
Applies the requirements for classifying, marking, redacting, handling, transporting, and safeguarding of protected and/or classified information.

COUNTERINTELLIGENCE
Gathers information and conducts activities to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities.

SECURITY TOOLS AND METHODS
Applies tools and methods to a substantive discipline, domain, or area of work. Adapts existing tools and/or methods or employs new methodological approaches required for the substantive discipline, domain, or area of work.

VULNERABILITIES ASSESSMENT AND MANAGEMENT

Conducts assessments on threats and vulnerabilities, determines the level of risk, and develops and recommends appropriate mitigation countermeasures in operational and non-operational situations. Conducts assessments in a counterintelligence context to protect against espionage; other intelligence activities; and sabotage conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities.

During this scenario, you will be asked questions about the following knowledge areas:

- Security Violations/Incidents
- JPAS
- SF-312
- Access/Eligibility requirements
- Risk Management
- Working with Counterintelligence (CI)
- Damage Assessments
- SCI information
- NATO information
- FGI information
- Destruction of classified information

Scenario 2

Cast

Roger: BAIT Program Manager
Mathew: BAIT Senior Test Engineer
Mitch: BAIT Senior Scientist
Mary Ann: a member of the Unit Compliance Inspection team
Unnamed: a foreign visitor

Brief Description of the Scenario

Scenario 2 discusses the BAIT (Best Airplane in Town) program. BAIT is a multi-engine, turbofan, wide-body, strategic airlift aircraft capable of stealthily moving combat equipment into and within austere theater environments. It is expected to provide significant improvements in both performance and operational costs compared to the aircraft in the current airlift fleet. In the first part of the scenario, Roger, the BAIT Program Manager, reports a security incident stemming from a conversation between two team members. The candidate will be given a copy of the BAIT Security Classification Guide to answer the questions to this scenario. In the second part of the scenario, Mary Ann, a member of the Unit Compliance Inspection team, learns that the BAIT's new radar system is based on a particular signature control technology included in the Military Critical Technology List (MCTL). The candidate will explore questions on the ramifications of this discovery. The final part of the scenario involves Mary Ann's discovery that a group of foreign academics visited the facility and gained access to an unclassified website. During the visit, one of the visitors seems to know a little more about the radar system than he or she should.

This scenario aligns to the following security competencies:

INFORMATION SECURITY
Applies knowledge of policies, procedures, and requirements established under appropriate authorities to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security.

INCIDENT RESPONSE
Responds to crisis or urgent situations including accidents; man-made, biological, chemical, radiological, or natural disasters; and other incidents that could result in harm to people, property, or the environment. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life and preservation of property.

CLASSIFICATION MANAGEMENT
Applies the requirements for classifying, marking, redacting, handling, transporting, and safeguarding of protected and/or classified information.

COUNTERINTELLIGENCE
Gathers information and conducts activities to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities.

OPERATIONS SECURITY
Analyzes unclassified, highly sensitive, and close-hold information to identify sensitive information that could adversely affect mission if revealed to those without a need to know. Advises on the protection of the unclassified, highly sensitive, and close-hold information.

PERSONNEL SECURITY
Applies personnel security principles and methods to process initial clearances, periodic re-investigations, clearance upgrades/downgrades, and to complete the adjudication and appeals processes. Evaluates internal and external security clearance requests and ensures applicants' actions are consistent with regulatory requirements. Analyzes and reports on clearances and appeals findings to senior security officials and makes appropriate notifications.

PROGRAM SECURITY
Employs an array of acquisition and contract security measures to sustain secrecy of highly sensitive U.S. government programs and/or activities. Prevents unauthorized disclosure of national intelligence program information throughout the contract lifecycle e.g., FOCI, connections with adversarial or terrorist organizations.

VULNERABILITIES ASSESSMENT AND MANAGEMENT
Conducts assessments on threats and vulnerabilities, determines the level of risk, and develops and recommends appropriate mitigation countermeasures in operational and non-operational situations. Conducts assessments in a counterintelligence context to protect against espionage; other intelligence activities; sabotage conducted for or on behalf of foreign powers, organizations or persons; or international terrorist activities.

During this scenario, you will be asked questions about the following knowledge areas:

- Security Violations/Incidents
- Following Security Classification Guidance
- Military Critical Technology List (MCTL)
- Acquisition Security
- OPSEC
- Risk Management
- Counterintelligence (CI)
- Technology Control Plan (TCP)

The purpose of the SAPPC Diagnostic tool is to familiarize candidates with scenarios, as well as topic areas that are assessed through the SAPPC. Please note that Security Fundamentals Professional Certification (SFPC) is a prerequisite to SAPPC. A candidate must hold the SFPC before becoming eligible to take SAPPC. For more information regarding SPēD Certification Program tools and resources, please visit: http://www.dss.mil/seta/sped/sped_what.html For more information on the ICD 610 Competencies, please visit: http://www.dni.gov/electronic_reading_room/ICD_610.pdf.