Security Fundamentals Professional Certification (SFPC)
Competency Preparatory Tools (CPT)

SFPC Experience Checkup | Please note: Cyber items are indicated with a ** at the end of the practice test questions.

Experience Statement	Linked Competency
1. Implement the classification decision process including establishing and/or sustaining the establishment of classification decision documentation (e.g., Security Classification Guides).	Info Sec
2. Review and respond to challenges to classification decisions and requests for downgrades.	Info Sec
3. Analyze and apply laws, standards, regulations, policies, requirements, and guidance associated with derivative classification of information.	Info Sec
4. Identify and analyze the protection requirements of special types of information (e.g., Restricted Data and Formally Restricted Data (RD/FRD), Foreign Government Information (FGI), Sensitive Security Information (SSI)). **	Info Sec & Cyber
5. Oversee the execution of controls and safeguards that prevent unauthorized access to classified information.	Info Sec
6. Oversee information disposition according to declassification and/or destruction requirements.	Info Sec
7. Advise on the application of information transmission requirements.	Info Sec
8. Classify information as outlined in applicable laws, standards, regulations, policies and requirements.	Info Sec
9. Designate control levels to controlled unclassified information as outlined in applicable laws, standards, regulations, policies and requirements.	Info Sec
10. Enforce proper handling of security incidents to ensure the effective implementation of established processes and procedures for reporting impact and/or damage resulting from security incidents.	Info Sec

Experience Statement	Linked Competency
11. Identify, interpret, initiate, and/or coordinate the implementation of the appropriate investigative and/or re-investigative process.	Pers Sec
12. Identify/interpret national security standards and criteria to determine eligibility.	Pers Sec
13. Apply knowledge and oversee the execution of physical security controls and safeguards that prevents unauthorized access to classified information.	Pers Sec
14. Utilize visitor notification processes and procedures to protect access to sensitive and/or classified information.	Indus Sec
15. Identify/interpret contractor eligibility (i.e., physical and logical access) standards and criteria.	Indus Sec
16. Identify, interpret, and/or address security requirements in contract documents and during the contracting process.	Indus Sec
17. Advise contractor personnel on establishing, implementing, and maintaining security programs for safeguarding classified information.	Indus Sec
18. Employ a systematic approach to address cyber security risks by providing guidance to the development of the System. Security Plans and/or Assessment and Authorization packages in accordance with Security Technical Implementation Guide (STIGs).**	Gen Sec & Cyber
19. Conduct the systematic assessment and evaluation of security risk by implementing security reviews, surveys, and inspections (including Command Cyber Readiness Inspections – CCRI).**	Gen Sec & Cyber
20. Evaluate risks to DoD assets by providing guidance in the determination, development, and execution of appropriate procedures and/or measures to mitigate identified risks to or due to introduction of new technology and equipment. **	Gen Sec & Cyber

Experience Statement	Linked Competency
19. Determine the security risk assessment and evaluation with the use of counterintelligence (CI) threat assessments.	Gen Sec
20. Utilize the five-step Operations Security (OPSEC) process to provide a security risk evaluation and assessment.	Gen Sec
21. Conduct briefings and debriefings that: (1) inform personnel of their security roles, responsibilities, and accountabilities; (2) make personnel aware of threats (general and/or specific) and/or (3) provide personnel procedures to address security concerns.	Gen Sec
22. Apply knowledge to: (1) specific requirements and the need for Security Education Training and Awareness (SETA); (2) prepare, disseminate, and/or implement SETA; and (3) monitor and evaluate impact of SETA initiatives.	Gen Sec
23. Evaluate the security risk, facilitate systematic analysis, and provide guidance to conduct loss, threat, and vulnerability assessments.	Gen Sec
24. Participate in Command Cyber Readiness Inspections (CCRI) execution. **	Gen Sec & Cyber