Security Asset Protection Professional Certification (SAPPC)
Competency Preparatory Tools (CPT)

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

Experience Statement	Linked Competency
1. Participate in the development and evaluation of assessment and authorization packages as it relates to cyber security.**	Info Sec & Cyber
2. Advise on the translating/applying the "need-to-know" criteria.	Info Sec
3. Employ the proper procedures for security incidents to ensure the effective implementation of established processes for identifying, evaluating, and reporting damage that resulted from the security incident.	Info Sec
4. Apply proper procedures for security incidents by ensuring implementation of established inquiry processes.	Info Sec
5. Provide guidance to the original classification decision process to ensure that (1) only authorized and trained personnel are making original classification decisions; and (2) original classification decisions abide with applicable executive orders, laws, standards, regulations, policies, and requirements.	Info Sec
6. Provide guidance to the implementation of the original classification decision process as it relates to the implementation of the declassification and re-grading policies and procedures.	Info Sec
7. Provide guidance on analyzing and applying executive orders, laws, standards, regulations, policies and requirements associated with derivative classification of information.	Info Sec
8. Provide technical guidance/direct support and monitor applications for marking classified products.	Info Sec
9. Apply guidance and support to identify and analyze Sensitive Compartmented Information (SCI) protection requirements.	Info Sec

Experience Statement	Linked Competency
10. Provide guidance and support to identify and analyze North Atlantic Treaty Organization (NATO) information protection requirements.	Info Sec
11. Provide guidance on the transmission and transportation requirements for sensitive unclassified and classified materials.	Info Sec
12. Apply knowledge of the national security clearance process and provide guidance to changes in personnel clearance status.	Pers Sec
13. Apply knowledge of the national security clearance process and provide continued support in the implementation of the Continuous Evaluation Program (CEP).	Pers Sec
14. Validate or recommend position sensitivity designations.	Pers Sec
15. Employ the personnel security process and monitor the implementation of the proper investigative and/or re-investigative process.	Pers Sec
16. Utilize visitor access control processes and procedures, as it relates to physical security, to prevent unauthorized entry to sensitive and classified work spaces or facilities.	Phys Sec
17. Apply knowledge of identification of relevant protection requirements, and coordinate the preparation and maintenance of the DD Form 254, Contract Security Classification Specification.	Indus Sec
18. Utilize visitor access control processes and procedures, as it relates to industrial security, to protect access to sensitive and/or classified information.	Indus Sec

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