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

Question	Answer	Linked Competency	Policy
1. What is the security professionals' role in pursuing and meeting cyber security goals?**	The role of the cyberspace workforce is to "secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions" (DoDD 8140.01). Per DoDI 8500.01, Cybersecurity (March 14, 2014), personnel occupying cybersecurity positions must be assigned in writing and trained / qualified in accordance with their role. The 080 position classification standards assigns them the responsibility of developing, implementing and monitoring policies and procedures, developing classification guides, destroying information, and performing oversight reviews to monitor program implementation.	Info Sec & Cyber	DoDI 8500.01
2. Explain the process for responding to a "spillage." **	The basic process under this requirement is: 1. Detection (implied) 2. Notification and preliminary inquiry 3. Containment and continuity of operations 4. Formal inquiry 5. Resolution 6. Reporting	Info Sec & Cyber	CJCSM 6510.01B
3. Describe the security professional's possible roles in handling a security incident.	a. Secure b. Safeguard c. Report d. Inquire e. Investigate	Info Sec	CJCSM 6510.01B

Question	Answer	Linked Competency	Policy
4. List three types of safeguarding procedures for classified information.	a. Proper storage b. Proper handling c. Approved disposition d. Proper transmission/transportation methods e. Receipt use, when required f. Dissemination g. Physical security measures h. Technical, administrative, and personnel control measures (deleted access control as these measures constitute access control) i. Develop emergency plan	Info Sec	• E.O13526 • DoD Manual 5200.01, Volumes 1, 2, 3 • ISOO32 CFR Parts 2001 & 2003, "Classified National Security Information Final Rule" • DoD 5200.2-R • DoD 5200.8-R, "Physical Security Program"
5. List three transmission and transportation requirements that help manage risks to DoD assets.	a. Safeguarding b. Briefings c. Documentation d. Personal control e. Pre-coordination f. Preparing for transportation (packaging) g. Utilizing proper methods of transmission/transportation based on classification level h. Intended recipients have proper clearance/eligibility and need to know (or access) i. Capability to properly store classified information	Info Sec	• E.O. 13526 • DoD Maunual 5200.01, Volume 3, Encl.4 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information Final Rule"
6. How does lack of attention to the concept of compilation of information introduce risks to DoD assets?	a. Unauthorized disclosure b. Misclassification c. Security Violation d. Improper safeguarding e. Improper dissemination f. Improper handling g. Improper destruction h. Data Spill	Info Sec	• E.O. 13526 • DoD Maunual 5200.01, "DoD Information Security Program" Volumes 1 & 3 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information Final Rule

Question	Answer	Linked Competency	Policy
7. List at least three individuals in the personnel security investigation (PSI) process and describe their roles.	a. Facility Security Officer/Security Manager/Security Officer/ Security Coordinator/Security Assistant: initiates, reviews, forwards E-Qip investigation to investigation service provider (ISP) b. Subject: Completes forms and provides additional information if required c. Investigator: Conducts PSI d. Adjudicator: Determines security clearance eligibility	Pers Sec	• DoD 5200.2-R • E.O. 12968
8. Explain how the adjudication process contributes to effective risk management of DoD assets.	a. Determines an individual's loyalty, reliability, and trustworthiness are in the best interest of national security.	Pers Sec	• DoD 5200-R, "Personnel Security Program" • White House Memorandum, "Revised Adjudicative Guidelines" • EO 12968 • EO 13467, Amendment to EO 12968
9. Explain how effective implementation of the continuous evaluation process contributes to management of the risks to DoD assets.	a. Ensures that individuals with security clearance eligibility and access are continuously assessed through utilization of accessible databases and other lawfully available information; continue to meet adjudicative standards; and that any issues that may arise are promptly reported and addressed.	Info Sec	• DoD 5200.2-R, • EO 12968 • EO 13467, Amendment to EO 12968 • EO 10450

Question	Answer	Linked Competency	Policy
10. List two factors that should be considered when determining position sensitivity.	a. Level of access to classified information b. IT level needed c. Duties associated with position	Pers Sec	• DoD 5200.2-R • EO 12968 • 5 CFR 731.106 Designation of public trust positions and investigative requirements • 5 CFR 832.201 Sensitivity level designation and investigative requirements
11. Describe how authorization of Limited Access Authority impacts risk to DoD assets.	a. Increases risk by allowing a foreign national access to classified information. b. Reduces risk by ensuring Foreign Nationals with a unique or unusual skills set have been properly investigated, adjudicated or vetted before being granted access to specific pieces of classified information only.	Pers Sec	• DoD 5200.2-R • EO 12968
12. Who determines or identifies when physical security surveys and inspections are required?	a. DoD Component Commanders b. Program Managers c. Security Managers d. Physical Security Specialists/Officers	Phys Sec	• DoDI 2000.12 • DoDI 2000.16, "DoD Antiterrorism (AT) Standards"
13. What is the difference between physical security surveys and physical security inspections?	a. A physical security survey is a formal record assessment of an installation's overall security posture; whereas a physical security inspection is a formal record of compliance of physical procedures and measures implemented by a unit or activity to protect its assets.	Phys Sec	• DoDI 5100.76, "Safegaurding Conventional Arms, Ammunition, and Explosives"

Question	Answer	Linked Competency	Policy
14. Explain how visitor identification control methods are used to effectively control access to facilities.	a. Ensure only authorized personnel and materials that enter and exit from an installation or facility are properly identified, verified, and authenticated.	Phys Sec	DoD 5200.08-R, "Physical Security Program
15. Explain why access control measures are contingent on Force Protection Conditions.	a. The Force Protection Conditions determine the amount of control measures needed to be taken in response to various levels of threats against military facilities or installations.	Phys Sec	• DoDI 2000.12 • DoDI 2000.16, "DoD Antiterroism (AT) Standards"
16. Identify the five Cognizant Security Agencies (CSAs) and describe their role in the National Industrial Security Program (NISP).	a. The five (5) CSAs are the Department of Defense, Director of National Intelligence, Department of Energy, Nuclear Regulatory Commission, Department of Homeland Security. b. Implement and oversee an Industrial Security Program to safeguard classified information with cleared industry under the respective CSA's jurisdiction.	Indus Sec	• DoD 5220.22-M, "National Industrial Security Program • Operating Manual" (NISPOM)*1-101, 1-104
17. Briefly describe the purpose of the DD Form 254	a. Convey security requirements and classification guidance, and provide handling procedures for classified materials received and/or generated under a classified contract.	Indus Sec	• Federal Acquisition Regulation (FAR), Subpart 4.4 • DoD 5220.22-M, "Nispom" • DoD 5220.22-R, Industrial Security Regulation C7 (entire)

Question	Answer	Linked Competency	Policy
18. List three (3) factors for determining whether US companies are under Foreign Ownership Control of Influence (FOCI).	a. Record of economic and government espionage against the US targets b. Record of enforcement/engagement in unauthorized technology transfer c. Type and sensitivity of the information that shall be accessed d. The source, nature and extent of FOCI e. Record of compliance with pertinent US laws, regulations and contracts f. Nature and bilateral and multilateral security and information exchange agreements g. Ownership or control in whole or part, by a foreign government	Indus Sec	• DoD 5220.22-M, "Nispom," 2-301 • DoD 5220-r, Industrial Security Regulation C2.23
19. List three different types of threats to classified information.	a. Insider threat b. Foreign Intelligence entities c. Cybersecurity Threat	Gen Sec	• DoDD 5240-.06, "CI Awareness and Reporting • DoDM 5200.01, Vol 3
20. List three elements that a security professional should consider when assessing and managing risks to DoD assets.	a. Asset b. Threat c. Vulnerability d. Risk e. Countermeasures	Gen Sec	• Enclosure 3 of DoDM 5200.01-V3, "Risk Assessment" • DoDM 5205.02

Question	Answer	Linked Competency	Policy
21. Describe the purpose of the Foreign Visitor Program.	a. To track and approve access by a foreign entity to information that is classified; and to approve access by a foreign entity to information that is unclassified, related to a US Government contract, or contractor/ government facility visits covered by International Traffic in Arms Regulations (ITAR).	Gen Sec	• NISPOM 10-507 • DoDI 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information" • DoDD 5230.02
22. What are at least three principle incidents/events required to be reported to DoD counterintelligence (CI) organizations?	a. Espionage b. Sabotage c. Terrorism d. Cyber e. Insider Threat	Gen Sec	• DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM" • EO 12333 • DoDI 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information"
23. List at least three indicators of insider threats.	a. Failure to report overseas travel or contact with foreign nationals b. Seeking to gain higher clearance or expand access outside the job scope c. Engaging in classified conversations without a need to know d. Working hours inconsistent with job assignment or insistence on working in private e. Exploitable behavior traits f. Repeated security violations g. Attempting to enter areas not granted access to h. Unexplained affluence/living above one's means i. Anomalies (adversary taking actions which indicate they are knowledgeable to information) j. Illegal downloads of information/files	Gen Sec	• EO 13587 • DoDI 5240.26, "Countering Espionage, International Terrorism and the Counterintelligence (CI) Insider Threat • DoDI5240-04, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA) • DoDi 5240-014, "Counterintelligence Investigations: • DoDD 5240-.06

Question	Answer	Linked Competency	Policy
24. Identify the three core components of the Risk Assessment process.	a. Asset criticality b. Threat Assessment c. Vulnerability Assessment	Gen Sec	• DoDI 2000.12 • DoDD 3020.40 • DoDI 3020.45
25. Define the purpose and function of the militarily critical technologies list (MCTL).	a. Serves as a technical reference for the development and implementation of DoD technology, security policies on international transfers of defense-related goods, services, and technologies as administered by the Director, Defense Technology Security Administration (DTSA). b. Formulation of export control proposals and export license review.	Gen Sec	• DoDI 3020.46, "The Military Critical Technologies List (MCTL) • Exportation Administration Act of 1979 (Extended by Executive Order) • Military Critical Technologies List
26. List the three categories of Special Access Programs.	a. Acquisition b. Intelligence c. Operations and support	Gen Sec	• DoDD 5205.07, "SAP Policy" • DoDI 5205.11, "Management, Administration, and Oversight of DoD Special Programs"
27. Briefly define a Special Access Program.	a. A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.	Gen Sec	EO 13526

Question	Answer	Linked Competency	Policy
28. List at least three (3) types of security briefings that help manage risks to DoD assets.	a. Initial orientation b. Annual refresher c. Threat awareness d. Foreign Travel e. Derivative classification f. Debriefings g. Termination briefing h. Counterintelligence briefing	Gen Sec	• EO 13256 • DoD Manual 5200.01, Volume 3, Encl 5 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Informational Final Rule" • DoD 5200.02-R, "Personnel Security Program"
29. Identify specific baseline administrative and/or physical security controls applicable to each system categorization. **	The CCRI process includes defining the scope, the inspection phase, documentation of observations, and reporting findings. A security professional would have responsibilities in defining the scope of the inspection, overseeing the self-inspection and remediation efforts, and coordinating with the CCRI team throughout the remainder of the process. The 080, for example, would ensure compliance with the established security program prior to the inspection, develop policies and procedures to close security gaps, ensure proper destruction and sanitization measures are in place. Dedicated cybersecurity workforce personnel would be directly responsible for scanning, patching, and other IT-related tasks. Per DoDI 8500.01, the CCRI requires a "unity of effort" between security disciplines, to include cybersecurity. A security professional will generally be assigned to oversee the CCRI process and assist the assessment team at each phase.		NIST SP 800-53