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

Question	Answer	Linked Competency	Policy
1. Describe two impacts of cybersecurity lapses on non-repudiation. **	Negative impacts if no non-repudiation: 1) Sender could deny the message was sent. 2) Recipient of an email could change the message and contest that the altered message was sent by the sender. **Definition:** Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.	Info Sec & Cyber	NIST SP 800-60
2. Describe two impacts of cybersecurity lapses on confidentiality**	Negative impacts if no confidentiality: 1) Persons could be granted access to information beyond their need-to-know. 2) Sensitive or classified information could be disclosed to an unauthorized system. **Definition:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	Info Sec & Cyber	• NIST SP 800-53 • FIPS 140-2
3. Define system categorization**	a. System Categorization is the process by which the Information Owner identifies the potential impact (low, moderate, or high) that would result from the loss of confidentiality, integrity, and availability should a security breach occur.	Info Sec & Cyber	NIST SP 800-37

Question	Answer	Linked Competency	Policy
4. Give three examples of data spills.**	a. Classified email sent to an unclassified network b. Classified document reproduced on an unclassified printer c. Classified document uploaded to an unclassified system d. Controlled unclassified information (CUI) transmitted without the required CUI protection and access controls	Info Sec & Cyber	• DoD Manual 5200.01 • CJCSM 6510.01B
5. List three duration/length/ declassification options for originally classified information.	Date or event that is a. Less than 10 years b. At 10 years c. Up to 25 years d. 50X1-HUM (with no date or event) e. 50X2-WMD (with no date or event) f. 25X (with a date or event)	Info Sec	• EO 13526 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information; Final Rule" • DoD Manual 5200.01, Volume 2, Encl 3 • DoDM 5200.01-V1, Encl 4
6. Define derivative Classification.	a. Incorporating, paraphrasing, restating or generating in a new form information that is already classified and marking the newly developed material consistent with the markings that apply to the source information.	Info Sec	• EO 13526 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information; Final Rule" • DoD Manual 5200.01, Volume 2, Encl 3 • DoDM 5200.01-V1, Encl 4

Question	Answer	Linked Competency	Policy
7. List three authorized sources of security classification guidance that could be used in the derivative classification process.	a. Security Classification Guide b. Properly Marked source document c. Contract Security Classification Specification (DD Form 254)	Info Sec	• EO 13526 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information; Final Rule" • Contract Security Classification Specification (DD Form 254) • DoDM 5200.45, "Instructions for Developing Classification Guides" • DoD Manual 5200.01, Volumes 2, Encl 3
8. List three main policies that govern the DoD Information Security Program.	a. E.O. 13526 b. Information Security Oversight Office (ISOO) 32 CFR Parts 2001 & 2003, Classified National Security Information; Final Rule" c. DoD Manual 5200.01, Volumes 1-4	Info Sec	• EO 13526 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information; Final Rule" • DoD Manual 5200.01, Volume 2, Encl 3 • DoDM 5200.01, Volumes 1-4
9. What must an "authorized person" have before being granted access to classified information?	a. Favorable determination of eligibility for access b. A need to know the information c. Signed SF 312 Nondisclosure Agreement	Info Sec	• EO 13526 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information; Final Rule" • DoD Manual 5200.01, Volume 2, Encl 3 • DoDM 5200.01, Volume 1, Encl 3
10. Define unauthorized disclosure.	a. Communication or physical transfer of classified or controlled unclassified information to an unauthorized recipient.	Info Sec	• EO 13526 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information; Final Rule" • DoD Manual 5200.01, Volume 2, Encl 3 • DoDM 5200.01, Volume 3, Encl 6

Question	Answer	Linked Competency	Policy
11. Define the difference between a security infraction and a security violation.	a. An infraction cannot reasonably be expected to and does not result in the loss, compromise, or suspected compromise of classified information; whereas a violation does result in or could be expected to result in the loss or compromise of classified information.	Info Sec	• EO 13526 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information; Final Rule" • DoD Manual 5200.01, Volume 2, Encl 3 • DoDM 5200.01, Volume 3, Encl 6
12. List three primary authorities governing foreign disclosure of classified military information.	a. Arms Export Control Act b. National Security Decision Memorandum 119 c. National Disclosure Policy – 1 d. International Traffic in Arms Regulation (ITAR) e. E.O.s 12829, 13526 f. Bilateral Security Agreements g. DoD 5220.22-M, "NISPOM"	Info Sec	• Arms Export Control Act • National Security Decision Memorandum 119 • National Disclosure Policy-1 • International Traffic in Arms Regulation (ITAR) • EO 12829 & 13526 • Bilateral Security Agreements • DoD 5220.22-M, "NISPOM"

Question	Answer	Linked Competency	Policy
13. List five adjudicative guidelines.	a. Allegiance to the US b. Foreign influence c. Foreign preference d. Sexual behavior e. Personal conduct f. Financial considerations g. Alcohol consumption h. Drug involvement i. Psychological conditions j. Criminal conduct k. Handling protected information l. Outside activities m. Use of information technology	Pers Sec	• White House Memorandum dated December 29, 2005, Subject: Adjudicative Guidelines • Under Secretary of Defense Memorandum dated August 20, 2006, Subject: Implementation of Adjudicative Guidelines for Determining Eligibility for Access to Classified Information • DoD 5200.2-R • EO 12968
14. Describe the purpose of due process in the Personnel Security Program (PSP).	a. Ensures fairness by providing the subject the opportunity to appeal an unfavorable adjudicative determination.	Pers Sec	• EO 12968 • DoD 5200.2-R
15. Describe the purpose of a Statement of Reason (SOR).	a. The purpose of the SOR is to provide a comprehensive and detailed written explanation of why a preliminary unfavorable adjudicative determination was made.	Pers Sec	• EO 12968 • DoD 5200.2-R
16. Describe the difference between revocation and denial in the Personnel Security Program (PSP).	a. Revocation: A current security eligibility determination is rescinded b. Denial: an initial request for security eligibility is not granted	Pers Sec	DoD 5200.2-R

Question	Answer	Linked Competency	Policy
17. List three DoD position sensitivity types and their investigative requirements	a. Critical Sensitive: Tier 5, Tier 5R b. Non-critical sensitive: Tier 3, Tier 3R c. Nonsensitive: Tier 1	Pers Sec	• DoD 5200.2-R • Federal Investigations Notice 12-07
18. List three types of initial personnel security investigations and to whom they apply.	a. Tier 5: Military, Civilian, Contractor b. Tier 3: Military, Civilian, Contractor c. Tier 1: Civilian and Contractor	Pers Sec	• Federal Investigations Notice 12-07 • DoD 5200.2-R • EO 13467 • EO 10450
19. List the key procedures for initiating Personnel Security Investigations (PSIs).	a. Validate the need for an investigation b. Initiate e-QIP c. Review Personnel Security Questionnaire (PSQ) for completeness d. Submit electronically to Office of Personnel Management (OPM)	Pers Sec	DoD 5200.2-R

Question	Answer	Linked Competency	Policy
20. List three enhanced security requirements for protecting Special Access Program (SAP) information.	a. All individuals with access to SAP are subject to a random counterintelligence-scope polygraph Access Rosters b. Polygraph examination, if approved by the DepSecDef, may be used as a mandatory access determination c. Tier review process d. Personnel must have a Secret or Top Secret Clearance e. SF-86 must be current within one year f. Limited Access g. Waivers required for foreign cohabitants, spouses, and immediate family members. **Industrial Security** a. The SecDef or DepSecDef can approve a carve-out provision to relieve Defense security service of industrial security oversight responsibilities. **Physical Security** a. Access control b. Maintain a SAP facility c. Access Roster d. All SAPs must have an unclassified nickname/codeword (optional). **Within Information Security** a. The use of Handled Via Special Access Channels Only (HVSACO). b. Transmission requirements (order of precedence)	Pers Sec	• DoDI 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs" • Department of Defense Overprint to the National Industrial Security Program Operating Manual Supplement -1, April 2004 • DoDD 5205.07, "SAP Policy"
21. What is the purpose of an Antiterrorism Program?	a. Protect personnel, their families, installations, facilities, information, and other material resources from terrorist acts.	Phys Sec	DoDI 2000.16, "Antiterrorism (AT) Standards"

Question	Answer	Linked Competency	Policy
22. List three Force Protection Condition levels.	a. Normal b. Alpha c. Bravo d. Charlie e. Delta	Phys Sec	• DoDI2000.16 • DoD-O 2000.12H, "DoD Antiterrorism Handbook: • DoDI 2000.12, "DoD Antiterrorism (AT) Program
23. What is the purpose of perimeter barriers?	a. Defines the physical limits of an installation, activity, or area, restrict, channel, impede access, or shield activities within the installation from immediate and direct observation.	Phys Sec	Unified Facilities Criteria 4-022-02
24. List three different physical means for approved classified storage.	a. General Services Administration (GSA)-approved storage containers b. Vaults (including modular vaults) c. Open storage area (secure rooms, to include sensitive compartmented information facility (SCIFs) and bulk storage areas)	Phys Sec	• DoD 5200.1, Volume 1-3 • DoDI 3224.03 • ICS 705-1 • SF700
25. List three construction requirements for vault doors.	a. General Services Administration (GSA)-approved Class 5 door b. Steel Door with tamper resistant hinge pins c. Constructed of metal d. Hung on non-removable hinge pins or with interlocking leaves e. Equipped with a GSA-approved combination lock f. Emergency egress hardware (deadbolt or metal bar extending across width of door)	Phys Sec	DoDM 5200.01, Volume 3

Question	Answer	Linked Competency	Policy
26. What is the purpose of intrusion detection systems?	a. Detect unauthorized penetration into a secured area.	Phys Sec	• DoDM 5200.01, Volume 3; Appendix to Volume 3 • DoDM 5100.76, "Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives
27. List three methods that can be applied by a cleared U.S. company to negate or mitigate the risk of foreign ownership or control.	a. Board Resolution b. Voting Trust Agreement c. Proxy Agreement d. Special Security Agreement (SSA) e. Security Control Agreement (SCA)	Indus Sec	• DoDM 5200.01, Volume 3; Appendix to Volume 3 • DoDM 5100.76, "Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives
28. Briefly describe the purpose of the DD Form 254.	a. Convey security requirements, security classification guidance, and provide handling procedures for classified materials received and/or generated on a classified contract.	Indus Sec	• Federal Acquisition Regulation (FAR), Subpart 4.4 • DoD 5220.22-M, "Nispom" • DoD 5220.22-R, "Industrial Security Reglation C7 (entire)
29. Identify the five Cognizant Security Agencies (CSAs) and describe their role in the National Industrial Security Program (NISP).	a. The five CSAs are the Department of Defense (DoD), Director of National Intelligence (DNI), Department of Energy (DOE), Department of Homeland Security (DHS) and Nuclear Regulatory Commission (NRC). b. Establish an industrial security program to safeguard classified information under its jurisdiction.	Indus Sec	• DoD 5220.22-M, "National Industrial Security Program • Operating Manual (Nispom) 1-101, 1-104 • EO 12829

Question	Answer	Linked Competency	Policy
30. List five responsibilities of the Government Special Access Program (SAP) Security Officer/ Contractor Program Security Officer (GSSO/ CPSO).	a. Ensure personnel processed for access to a SAP meet the prerequisite personnel clearance and/or investigative requirements specified b. Ensure adequate secure storage and work spaces c. Ensure strict adherence to provisions of the National Industrial Security Program Operating Manual (NISPOM), its supplement, and the Overprint d. When required, establish and oversee a classified materials control program for each SAP e. When required, conduct an annual inventory of accountable classified materials f. When required, establish a Special Access Program Facility (SAPF) g. Establish and oversee a visitor control program h. Monitor reproduction and/or duplication and destruction capability of SAP information i. Ensure adherence to special communications capabilities within the SAPF j. Provide for initial program indoctrination of employees after their access is approved; rebrief and debrief personnel as required k. Establish and oversee specialized procedures for the transmission of SAP materials to and from Program elements l. When required, ensure contractual specific security requirements such as TEMPEST Automated information system (AIS), and operation security (OPSEC) are accomplished m. Establish security training and briefings specifically tailored to the unique requirements of the SAP	Indus Sec	Revision 1, Department of Defense Overprint to the National Industrial Security Program Operating Manual Supplement -1 April 2004

Question	Answer	Linked Competency	Policy
31. List 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 Access Programs"
32. 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
33. What are three principle incidents/ events required to be reported to DoD counterintelligence (CI) organizations?	a. Espionage b. Sabotage c. Terrorism d. Cyber Intrusion	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"
34. List three different types of threats to classified information.	a. Insider threat b. Foreign Intelligence entities c. Cybersecurity Threat	Gen Sec	• EO 13587 • DoDI 5240.26, Countering Espionage, International Terrorism and the Counterintelligence (CI) Insider Threat: • DoDI 5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)" • DoDI 5240.04, "Counterintelligence (CI) Investigations" • DODD 5240.06

Question	Answer	Linked Competency	Policy
35. List three indicators of insider threat.	a. Working hours inconsistent with job assignment or insistence on working in private b. Exploitable behavior traits c. Repeated security violations d. Attempting to enter areas not granted access to e. Unexplained affluence/living above one's means f. Anomalies (taking actions which indicate they are knowledgeable of information) g. Illegal downloads of information/files	Gen Sec	• EO 13587 • DoDI 5240.26, "Countering Espionage, International Terrorism and the Counterintelligence (CI) Insider Threat • DoDI 5240.26, Countering Espionage, International Terrorism and the Counterintelligence (CI) Insider Threat: • DoDI 5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)" • DoDI 5240.04, "Counterintelligence (CI) Investigations" • DODD 5240.06
36. Briefly describe the concept of insider threat.	a. An employee who may represent a threat to national security. These threats encompass potential espionage, violent acts against the Government or the nation, and unauthorized disclosure of classified information, including the vast amounts of classified data available on interconnected US Government computer networks and system.	Gen Sec	• EO 13587, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs" • DoDI 5240.26, "Counterintelligence, Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat"

Question	Answer	Linked Competency	Policy
37. List three elements that should be considered in identifying critical program information.	Element which if compromised could: a. Cause significant degradation in mission effectiveness b. Shorten the expected combat-effective life of the system c. Reduce technological advantage d. Significantly alter program direction e. Enable an adversary to defeat, counter, copy, or reverse-engineer the technology or capability	Gen Sec	DoDI 52009.39, "Critical Program Information (CPI) Protection Within the Department of Defense"
38. Which DoD instructions outline the Assessment and Authorization process? **	a. The Risk Management Framework (RMF) process leads to Assessment and Authorization. DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology, and DoD 8500.01, Cybersecurity, outlines the Assessment and Authorization policies and processes.	Gen Sec & Cyber	DoDI 8510.01
39. What are the steps in the Risk Management Framework (RMF). **	a. Categorize Information System (IS) b. Select Security Controls c. Implement Security Controls d. Assess Security Controls e. Authorize f. Monitor Security Controls	Gen Sec & Cyber	DoDI 8510.01

Question	Answer	Linked Competency	Policy
40. List vulnerabilities related to the occurrence of a cyber security event. **	a. Security controls not properly applied, existing controls becoming inadequate over time, outdated technologies, poorly configured devices, etc.	Gen Sec	DoDI 8500.01
41. What is the relationship between security control baselines and system categorization? **	a. Security controls are implemented based on the system's categorization. Specifically, once the security category of the information system is determined, organizations begin the security control selection process, selecting the baseline security controls corresponding to the security category of the system.	Gen Sec	NIST SP 800-53
42. Define security control baselines.**	a. A set of minimum security controls defined for a low, moderate, or high impact information system.	Gen Sec & Cyber	NIST SP 800-53

Question	Answer	Linked Competency	Policy
43. What are the eighteen security control families? **	a. For ease of use in the security control selection and specification process, controls are organized into nineteen families. Each family contains security controls related to the general security topic of the family. • Access Control • Awareness and Training • Audit and Accountability • Security Assessment and Authorization • Configuration Management • Contingency Management • Contingency Planning • Identification and Authentication • Incident Response • Maintenance • Media Protection • Physical and Environmental Protection • Planning • Personnel Security • Risk Assessment • System and Service Acquisition • System and Communications Protection • System and Information Integrity • Program Management	Gen Sec & Cyber	DoDI 8510.01

Question	Answer	Linked Competency	Policy
44. Identify the five essential components of cybersecurity. **	a. Confidentiality b. Integrity c. Availability d. Authentication e. Non-repudiation	Gen Sec & Cyber	NIST SP 800-33
45. Describe the following cyber security principles critical to the protection of information and information networks: least privilege, defense-in-depth, situational awareness. **	a. Least privilege: The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. b. Situational Awareness: Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future. c. Defense-in-depth: Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.	Gen Sec & Cyber	NIST SP 800-14
46. 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	• DoDM 5200.01, Volume 3, Encl 3, "Risk Assessment • DoDM 5205.02

Question	Answer	Linked Competency	Policy
47. Define each step of the Risk Management Framework (RMF).**	**Step 1: Categorize Information System (IS)** • Categorize the system in accordance with the CNSSI 1253 • Initiate the Security Plan • Register system with DoD Component Cybersecurity Program • Assign qualified personnel to RMF roles **Step 2: Select Security Controls** • Common Control Identification • Select security controls • Develop system-level continuous monitoring strategy • Review and approve the security plan and continuous monitoring strategy • Apply overlays and tailor **Step 3: Implement Security Controls** • Implement control solutions consistent with DoD Component Cybersecurity architectures • Document security control implementation in the security plan **Step 4: Assess Security Controls** • Develop and approve Security Assessment Plan • Assess security controls • SCA prepares Security Assessment Report (SAR) • Conduct initial remediation actions. **Step 5: Authorize** • Prepare the plan of action and milestones (POA&M) • Submit Security Authorization Package (security plan, SAR and POA&M) to authorizing official (AO) • AO conducts final risk determination • AO makes authorization decision	Gen Sec & Cyber	DoDI 8510.01