SFPC Knowledge Test Review Sheet

General Security

Question	Answer	Policy	Resource
What are three principle incident/ events required to be reported to DoD counterintelligence (CI) organizations?	• Espionage • Sabotage • Terrorism • Cyber	• DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)" • E.O. 12333 • DoDI 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information"	• NISPOM 1-302b or 1-301 • DoDI 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information • DoDD 5240.06, "CI Awareness and Reporting" • "Counterintelligence Awareness and Reporting Course for DoD Employees" CI116.06 • "Integrating CI and Threat Awareness into Your Security Program" CI010.06 • "NISP Reporting Requirements" IS150.16
List three indicators of insider threats.	• Failure to report overseas travel or contact with foreign nationals • Seeking to gain higher clearance or expand access outside the job scope • Engaging in classified conversations without a need to know • Working hours inconsistent with job assignment or insistence on working in private • Exploitable behavior traits • Repeated security violations • Attempting to enter areas not granted access to • Unexplainable affluence/living above one's means • Anomalies (adversary taking actions which indicate they are knowledgeable to information) • Illegal downloads of information/files	• E.O. 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	• "Counterintelligence Awareness and Reporting Course for DoD Employees" CI116.06 • "Thwarting the Enemy: Providing Counterintelligence & Threat Awareness to the Defense Industrial Base" CI111.16 • "Integrating CI and Threat Awareness into Your Security Program" CI010.16

General Security

Question	Answer	Policy	Resource
List three elements that should be considered in identifying Critical Program Information.	Elements which if compromised could: (1) cause significant degradation in mission effectiveness, (2) shorten the expected combat-effective life of the system; (3) reduce technological advantage; (4) significantly alter program direction; or (5) enable an adversary to defeat, counter, copy, or reverse-engineer the technology or capability.	• DoDI 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense"	• Defense Acquisition University (DAU)
List three elements that a security professional should consider when assessing and managing risks to DoD assets.	• Asset • Threat • Vulnerability • Risk • Countermeasures	• Enclosure 3 of DoDM 5200.01-V3, "Risk Assessment" • DoDM 5205.02	• "Risk Management for DoD Security Programs" GS102.16
List three categories of Special Access Programs.	• Acquisition • Intelligence • Operations and Support	• DoDD 5205.07, "SAP Policy" • DoDI 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs"	• "SAP Overview" SA001.16 • Security Short, "SAP Types and Categories"

General Security

Question	Answer	Policy	Resource
List three different types of threats to classified information.	(1) Insider Threat (2) Foreign Intelligence Entities (FIE) (3) Cybersecurity Threat	• DoDD 5240.06, "CI Awareness and Reporting" • DoDM 5200.01, Vol 3	• "Introduction to Information Security" IF011.16 • "Cybersecurity Awareness" CI130.16 • CDSE-hosted Course JC-CI101.06 "Insider Threat"
Briefly describe the concept of insider threat.	• 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 United States Government computer networks and systems.	• E.O. 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"	• JCITA Insider Threat Course • "Integrating CI and Threat Awareness Into Your Security Program" C1010.16 • "Cybersecurity Awareness" CI1630.16 • CDSE-hosted e-Learning Course "Cyber Awareness Challenge" • "Counterintelligence Awareness and Reporting Course for DoD Employees" CI116.06
Describe the purpose of the Foreign Visitor Program.	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 U.S. Government contract, or plant visits covered by ITAR.	• NISPOM 10-507 • DoDI 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information" • DoDD 5230.02	IS105.16, "Visits and Meeting in the NISP"
Briefly define a Special Access Program.	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.	E.O. 13526	"SAP Overview" SA001.16

General Security

Question	Answer	Policy	Resource
List three enhanced security requirements for protecting Special Access Program (SAP) Information.	**Within Personnel Security:** • Access Rosters; • Billet Structures (if required); • Indoctrination Agreement; • Clearance based on an appropriate investigation completed within the last 5 years; • Individual must materially contribute to the program in addition to having the need to know; • All individuals with access to SAP are subject to a random counterintelligence-scope polygraph examination; • Polygraph examination, if approved by the DepSecDef, may be used as a mandatory access determination; • Tier review process; • Personnel must have a Secret or Top Secret clearance; • SF-86 must be current within one year; • Limited Access; • Waivers required for foreign cohabitants, spouses, and immediate family members. **Within Industrial Security:** The SecDef or DepSecDef can approve a carve-out provision to relieve Defense Security Service of industrial security oversight responsibilities. **Within Physical Security:** • Access Control; • Maintain a SAP Facility; • Access Roster; • All SAPs must have an unclassified nickname/ Codeword (optional). **Within Information Security:** • The use of HVSACO; • Transmission requirements (order of precedence).	• 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"	• "SAP Overview" SA001.16 • Security Shorts, "SAP Types and Categories" • "Introduction to Special Access Programs" SA101.01

Industrial Security

Question	Answer	Policy	Resource
List five responsibilities of the Government SAP Security Officer/ Contractor Program Security Officer (GSSO/ CPSO)	**From Revision 1 Department of Defense Overprint to the National Industrial Security Program Operating Manual Supplement - 1 April 2004:** • Possess a personnel clearance and Program access at least equal to the highest level of Program classified information involved. • Provide security administration and management for his/her organization. • Ensure personnel processed for access to a SAP meet the prerequisite personnel clearance and/or investigative requirements specified. • Ensure adequate secure storage and work spaces. • Ensure strict adherence to the provisions of the NISPOM, its supplement, and the Overprint. • When required, establish and oversee a classified material control program for each SAP. • When required, conduct an annual inventory of accountable classified material. • When required, establish a SAPF. • Establish and oversee a visitor control program. • Monitor reproduction and/or duplication and destruction capability of SAP information • Ensure adherence to special communications capabilities within the SAPF. • Provide for initial Program indoctrination of employees after their access is approved; rebrief and debrief personnel as required. • Establish and oversee specialized procedures for the transmission of SAP material to and from Program elements • When required, ensure contractual specific security requirements such as TEMPEST Automated Information System (AIS), and Operations Security (OPSEC) are accomplished. • Establish security training and briefings specifically tailored to the unique requirements of the SAP.	• Revision 1 Department of Defense Overprint to the National Industrial Security Program Operating Manual Supplement - 1 April 2004	• "SAP Overview" SA001.16

Industrial Security

Question	Answer	Policy	Resource
Identify the four Cognizant Security Agencies (CSAs) and describe their role in the National Industrial Security Program (NISP).	The four CSAs are the Department of Defense (DoD), the Director of National Intelligence (DNI), the Department of Energy (DoE), and the Nuclear Regulatory Commission (NRC). Establish an industrial security program to safeguard classified information under its jurisdiction.	• DoD 5220.22-M, "National Industrial Security Program • Operating Manual (NISPOM)" 1-101, 1-104 • EO 12829, "National Industrial Security Program"	• "Introduction to Industrial Security" IS011.16
What is the definition of Critical Program Information in DoD?	• U.S. capability elements that contribute to the warfighter's advantage throughout the life cycle, which if compromised or subject to unauthorized disclosure, decrease the advantage. • Elements or components of a Research, Development, and Acquisition (RDA) program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. Includes information about applications, capabilities, processes and end-items. Includes elements or components critical to a military system or network mission effectiveness. Includes technology that would reduce the U.S. technological advantage if it came under foreign control.	• DoDI 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense"	• DoD 5200.39

Industrial Security

Question	Answer	Policy	Resource
List three primary authorities governing foreign disclosure of classified military information.	• Arms Export Control Act • National Security Decision Memorandum 119 • National Disclosure Policy-1 • International Traffic in Arms Regulation (ITAR) • E.O.s 12829, 13526 • Bilateral Security Agreements • DoD 5220.22-M, "NISPOM,"	• Arms Export Control Act • National Security Decision Memorandum 119 • National Disclosure Policy-1 • International Traffic in Arms Regulation (ITAR) • E.O.s 12829, 13526 • Bilateral Security Agreements • DoD 5220.22-M, "NISPOM,"	• DISAM International Programs Security Requirements IPSR-OLL IN112.06
Briefly describe the purpose of the DD Form 254.	• Convey security requirements, classification guidance and provide handling procedures for classified material received and/or generated on a classified contract.	• Federal Acquisition Regulation (FAR) Subpart 4.4 • DoD 5220.22-M, "NISPOM," • DoD 5220.22-R, Industrial Security Regulation C7 (entire)	• CDSE Job Aid, "How to Complete DD 254 Performance Support Guide"

Industrial Security

Question	Answer	Policy	Resource
List three factors for determining whether U.S. companies are under Foreign Ownership, Control or Influence (FOCI).	• Record of economic and government espionage against the U.S. targets • Record of enforcement/engagement in unauthorized technology transfer • Type and sensitivity of the information that shall be accessed • The source, nature and extent of FOCI • Record of compliance with pertinent U.S. laws, regulations and contracts • Nature of bilateral & multilateral security & information exchange agreements • Ownership or control, in whole or part, by a foreign government	• DoD 5220.22-M, "NISPOM," 2-301 • DoD 5220.22-R, Industrial Security Regulation C2.2.3	"Understanding Foreign Ownership, Control, or Influence (FOCI)" IS065.16
Define the purpose and the function of the Militarily Critical Technologies List (MCTL).	• 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). • Formulation of export control proposals and export license review	• DoDI 3020.46, "The Militarily Critical Technologies List (MCTL)" • Export Administration Act of 1979 (extended by Executive Order) • Militarily Critical Technologies List	• www.acq.osd.mil/rd/tech_security/mctp/mctl.html

Information Security

Question	Answer	Policy	Resource
List the three main policies that govern the DoD Information Security Program.	• E.O. 13526 • Information Security Oversight Office (ISOO) 32 CFR Parts 2001 & 2003, "Classified National Security Information; Final Rule" • DoD Manual 5200.01, Volumes 1-4	• E.O. 13526 • ISOO32 CFR Parts 2001 & 2003, "Classified National Security Information; Final Rule" • DoD Manual 5200.01, Volumes 1-4, "DoD Information Security Program"	• CDSE Resources Page • Defense Technical Information Center (www.dtic.mil) • "Information Security Management Course" IF201.01 • "Introduction to Information Security" IF011.16 • "Programs, Policies and Principles Course" GS140.16 • ISOO.gov • Archives.gov
What must an "authorized person" have before being granted access to classified information?	Have: • Favorable determination of eligibility for access • A need to know the information • Signed SF 312 Nondisclosure Agreement	• E.O. 13526 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information, Final Rule" • DoD Manual 5200.01, Volume 1 Encl. 3	• E.O. 13526 • DoDM 5200.01 Vol 1-4 • "Introduction to Information Security" IF011.16 • DoD 5200.2-R "Personnel Security Program" • ISOO.gov • SF312 • "Introduction to Personnel Security Course" PS113.16 • CDSE Resource Page- Personnel Security; General Security; Information Security
List three classification duration options for originally classified information.	• Date or event that is: • Less than 10 years • At 10 years • Up to 25 years • 50X1-HUM (with no date or event) • 50X2-WMD (with no date or event) • 25X (with a date or event)	• E.O. 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	• E.O. 13526 • ISOO.gov • DoDM 5200.01 Vol 1-4 • "Introduction to Information Security" IF011.16 • "Original Classification" IF102.16 • "Security Classification Guidance" IF101.16 • "Marking Classified Information" IF105.16 • CDSE Security Short, "Downgrading and Declassification" • "DoD Security Specialist" FS101.01 • "Information Security Management" IF102.01 • CDSE Resources Job aids

Information Security

Question	Answer	Policy	Resource
List three authorized sources of security classification guidance that could be used in the derivative classification process.	• Security Classification Guide • Properly Marked Source Document • Contract Security Classification Specification (DD Form 254)	• Executive Order 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 Security Classification Guides" • DoD Manual 5200.01, Volume 2, Encl. 3	• E.O. 13526 • ISOO, 32 CFR Parts 2001 & 2003 • DoDM 5200.01, Vol 1-4 • DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)" • DoDM 5200.45, "Instructions for Developing Security Classification Guides" • "Introduction to Information Security" IF011.06 • DTIC (www.dtic.mil) Website (electronic database for SCGs) • "Security Classification Guide" IF101.16 • CDSE Security Short, "DD Form 254"
Define derivative classification.	• Incorporating, paraphrasing, restating, or generating in new form information that is already classified and marking the newly developed material consistent with the markings that apply to the source information.	• E.O. 13526, "Classified National Security Information" • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information; Final Rule" • DoD Manual 5200.01, Volume 1, Encl. 4	• E.O. 13526 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information; Final Rule" • DoD Manual 5200.01, Volume 1, Encl. 4 • "Derivative Classification" IF011.16 • "DoD Security Specialist" GS101.01 • " Information Security Management" IF201.01 • CDSE Resources Jobaids (Derivative Classification) • DTIC training Website (CDSE training)

Information Security

Question	Answer	Policy	Resource
Define the difference between a security infraction and a security violation.	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.	• E.O. 13526 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information; Final Rule" • DoD Manual 5200.01, Volume 3, Encl. 6	• "Introduction to Information Security" IFO11.15 • E.O. 13526 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information; Final Rule" • DoD Manual 5200.01, Volume 3, Encl. 6 • National Counterintelligence Executive (NCIX.gov) - "Unauthorized Disclosure Course" • "ISM / DoD Security Specialist Course" IF201.01 • CDSE Security Shorts - "Security Incident Reporting Requirements "
Define unauthorized disclosure.	• Communication or physical transfer of classified or controlled unclassified information to an unauthorized recipient.	• E.O. 13526 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information; Final Rule" • DoD Manual 5200.01, Volume 3, Encl. 6	• "Introduction to Information Security" IFO11.15 • E.O. 13526 • ISOO 32 CFR Parts 2001 & 2003, "Classified National Security Information; Final Rule" • DoD Manual 5200.01, Volume 3, Encl. 6 • National Counterintelligence Executive (NCIX.gov) - "Unauthorized Disclosure Course" • "ISM / DoD Security Specialist Course" IF201.01 • CDSE Security Shorts - "Security Incident Reporting Requirements"

Personnel Security

Question	Answer	Policy	Resource
List three types of initial personnel security investigations and to whom they apply.	• SSBI: Military, Civilian, Contractor • ANACI: Civilian • NACLC: Military and Contractor • NACI: Civilian and Contractor	• Federal Investigations Notice 12-07 • DoD 5200.2-R, "DoD Personnel Security Program, with Changes 1,2,3" • E.O. 13467 • E.O. 10450	• "Introduction to Personnel Security" PS113.16 • "DoD Personnel Security Management for Security Professionals" PS212.01 • "Introduction to DoD Personnel Security Adjudications" 001.18
Describe the purpose of due process in Personnel Security Program (PSP).	Ensures fairness by providing the subject the opportunity to appeal an unfavorable adjudicative determination.	• E.O. 12968 • DoD 5200.2-R	• "DoD Personnel Security Management for Security Professionals" PS212.01 • PERSEREC Adjudicative Desk Reference
List the key procedures for initiating Personnel Security Investigations (PSIs).	• Validate the need for an investigation • Initiate e-QIP • Review Personnel Security Questionnaire (PSQ) for completeness • Submit electronically to OPM	DoD 5200.2-R	• OPM e-QiP Web-Based Training • "Introduction to Personnel Security" PS113.16 • "Introduction to DoD Personnel Security Adjudications" 001.18 • "DoD Personnel Security Management for Security Professionals" PS212.01
List three DoD position sensitivity types and their investigative requirements.	• Critical Sensitive: SSBI, SSBI-PR, PPR • Non-Critical Sensitive: ANACI, NACLC • Nonsensitive: NACI	• DoD 5200.2-R • Federal Investigations Notice 12-07	• "Introduction to Personnel Security" PS113.16 • "DoD Personnel Security Management for Security Professionals" PS212.01
Describe the difference between revocation and denial in Personnel Security Program (PSP).	• Revocation: A current security eligibility determination is rescinded. • Denial: An initial request for security eligibility is not granted.	DoD 5200.2-R	• "Introduction to Personnel Security" PS113.16 • "DoD Personnel Security Management for Security Professionals" PS212.01

Personnel Security

Question	Answer	Policy	Resource
Describe the purpose of a Statement of Reason (SOR).	The purpose of the SOR is to provide a comprehensive and detailed written explanation of why a preliminary unfavorable adjudicative determination was made.	• DoD 5200.2-R • E.O. 12968	• "DoD Personnel Security Management for Security Professionals" PS212.01 • PERSEREC Adjudicative Desk Reference
List five adjudicative guidelines.	• Allegiance to the United States • Foreign Influence • Foreign Preference • Sexual Behavior • Personal Conduct • Financial Considerations • Alcohol Consumption • Drug Involvement • Psychological Conditions • Criminal Conduct • Handling Protected Information • Outside Activities • Use of Information Technology Systems	• White House Memo dated December 29, 2005, Subject: Adjudicative Guidelines • Under Secretary of Defense Memo dated August 20, 2006, Subject: Implementation of Adjudicative Guidelines for Determining Eligibility for Access to Classified Information • DoD 5200.2-R • EO 12968	• Adjudicators Desktop Reference • CDSE: 13 Adjudicative Guideline Shorts • "Introduction to Personnel Security" PS113.16 • "DoD Personnel Security Management for Security Professionals" PS212.01 • "Introduction to DoD Personnel Security Adjudications" 001.18

Physical Security

Question	Answer	Policy	Resource
List three different types of approved classified material storage areas.	• GSA-approved storage containers • Vaults (including modular vaults) • Open storage area (secure rooms, to include SCIFs and bulk storage areas)	• DoDM 5200.01, Vol 3, "DoD Information Security Program"	• Information security short, "Classified Storage Requirements" • "Storage Containers and Facilities" PY 105.16
List three construction requirements for vault doors.	• Constructed of metal • Hung on non-removable hinge pins or with interlocking leaves. • Equipped with a GSA-approved combination lock. • Emergency egress hardware (deadbolt or metal bar extending across width of door).	DoDM 5200.01, Vol 3	• Information security short, "Classified Storage Requirements" • "Storage Containers and Facilities" PY105.16 • DoD Lock Program (https://locks.navfac.navy.mil); (1-800-290-7607 or DSN 551-1212)
What is the purpose of intrusion detection systems?	• Detect unauthorized penetration into a secured area	• DoDM 5200.01 V3, Appendix to Enclosure 3 • DoDM 5100.76, "Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives"	• "Physical Security Measures" PY103.16 • "Introduction to Physical Security" PY 011.06
What is the purpose of perimeter barriers?	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.	• Unified Facilities Criteria 4-022-02	• "Physical Security Measures" PY103.16 • "Physical Security Planning and Implementation" PY106.16

Physical Security

Question	Answer	Policy	Resource
What is the purpose of an Antiterrorism Program?	Protect DoD personnel, their families, installations, facilities, information, and other material resources from terrorist acts.	• DoDI 2000.16, "Antiterrorism (AT) Standards"	• "Introduction to Physical Security" PY011.06, • "Physical Security Planning and Implementation" PY106.16 • "Antiterrorism Officer (ATO) Level 2 Course" GS109.CU • CDSE Security Short "Antiterrorism Force Protection"
List three Force Protection Condition levels.	Normal, Alpha, Bravo, Charlie, Delta	• DoDI 2000.16 • DoD-O 2000.12-H, "DoD Antiterrorism Handbook" • DoDI 2000.12, "DoD Antiterrorism (AT) Program"	• "Introduction to Physical Security" PY011.06 • "Physical Security Planning and Implementation" PY106.16 • "Antiterrorism Officer (ATO) Level 2 Course" GS109.CU • CDSE Security Short "Antiterrorism Force Protection"
Describe the concept of security-in-depth.	Layered and complementary security controls sufficient to deter, detect, and document unauthorized entry and movement within an installation or facility.	• DoD 5200.08-R, "Physical Security Program"	• "Physical Security Measures" PY103.16 • "Introduction to Physical Security" PY011.06 • "Physical Security Planning and Implementation" PY106.16

All courses are CDSE unless otherwise indicated.