Objectives Sheet

ENG 260 - Program Protection for Practitioners

Course Learning/Performance Objectives followed by enabling learning objectives

ENG 260.U01.01	**Summarize the fundamentals of Program Protection Planning.**
ENG 260.U01.01.01	Recognize system security threats and consequences to acquisition programs
ENG 260.U01.01.02	Recognize that the system security solution approach includes risk-based prevention, detection and response to system security threats and vulnerabilities.
ENG 260.U01.01.03	Define how and when program protection is incorporated into the system requirements, statement of work and RFP for contracting.
ENG 260.U01.01.04	Recognize mission critical functions to achieve trusted system and network threat definitions, associated attacks and policy and guidance.
ENG 260.U01.01.05	Given DoDI 5000.02 recognize the requirement of the Program Protection Plan (PPP) within the acquisition life cycle.
ENG 260.U01.01.06	Given DoD Manual 5200.01 volumes 1-4, recognize the policy and criteria for classification of information and identification of information of Controlled Unclassified Information (CUI).
ENG 260.U01.01.07	Recognize the changing functional responsibilities and methods for program protection during the Operations & Support (O&S) phase of the system.
ENG 260.U02.01	**Apply Critical Program Information (CPI) analysis to acquisition lifecycle scenarios and DoDI 5000.02 models.**
ENG 260.U02.01.01	Summarize the cybersecurity, HWA, SWA, AT, Supply chain, DEF, and security specialties policy requirements and relationship to Program Protection, system design and the acquisition lifecycle (ENG 160 TLO 9 no new content).
ENG 260.U02.01.02	Demonstrate the impact of security specialties on Program Protection requirements, system design and system acquisition.
ENG 260.U02.01.03	Demonstrate the impact of cybersecurity policy on Program Protection requirements, system design and system acquisition.
ENG 260.U02.01.04	Demonstrate the impact of hardware assurance (HWA) on Program Protection requirements, system design and system acquisition.
ENG 260.U02.01.05	Demonstrate the impact of software assurance (SWA) policy and guidance on Program Protection requirements, system design and system acquisition.
ENG 260.U02.01.06	Demonstrate the impact of anti-tamper policy on Program Protection requirements, system design and system acquisition.
ENG 260.U02.01.07	Demonstrate the impact of supply chain risk management (SCRM) on Program Protection requirements, system design and system acquisition.
ENG 260.U02.01.08	Demonstrate the impact of Defense Exportability (DEF) on Program Protection requirements, system design and system acquisition.
ENG 260.U03.01	**Apply analyses to protect mission-critical functions to acquisition lifecycle scenarios and applicable DoDI 5000.02 models.**
ENG 260.U03.01.01	Summarize the purpose and methodology of the CPI analysis process for identification and protection of CPI.
ENG 260.U03.01.02	Identify potential threats, given generic threat information for acquisition program scenarios.
ENG 260.U03.01.03	Complete a CPI risk assessment, given acquisition program and operational scenarios.
ENG 260.U03.01.04	Explain the system security engineering specialties and security specialties that are applicable to CPI analysis and associated protection measures for each specialty.
ENG 260.U03.01.05	Explain the required horizontal protection processes.
ENG 260.U03.01.06	Recognize characteristics of CPI monitoring.
ENG 260.U03.01.07	Describe how CPI analysis is tailored for relevant Interim DoDI 5000.02 acquisition models.
ENG 260.U04.01	**Apply analyses to protect mission-critical functions to acquisition lifecycle scenarios and applicable DoDI 5000.02 models.**
ENG 260.U04.01.01	Summarize the purpose and methodology of the TSN Analysis for protection of mission-critical functionality, and its relationship to program protection.
ENG 260.U04.01.02	Apply criticality analysis to identify mission-critical functions and/or critical subsystems, and /or critical components, given a set of program and system information for acquisition program scenarios.
ENG 260.U04.01.03	Perform vulnerability analysis techniques given a set of program and system information for acquisition program scenarios.
ENG 260.U04.01.04	Identify potential threats, given generic threat information and supplier threat inputs for acquisition program scenarios.
ENG 260.U04.01.05	Describe how TSN analysis for protection of mission-critical functionality is tailored for different points in the acquisition life cycle.
ENG 260.U05.01	**Explain the elements of identifying and protecting classified and unclassified information within an acquisition program (include National Industrial Security. Program Operating Manual (NISPOM), DFARS and DSS).**
ENG 260.U05.01.01	Summarize the policy and requirements for protecting classified information and unclassified information.
ENG 260.U05.01.02	Summarize the purpose of the NISPOM, and the role of Defense Security Services (DSS).
ENG 260.U05.01.03	Explain program activities to identify and protect information across the lifecycle.
ENG 260.U05.01.04	Explain industry activities to identify and protect information across the lifecycle.
ENG 260.U05.01.05	Explain test and evaluation criteria for verification and validation of program protection risk protection measures and mitigations.

Objectives Sheet

ENG 260 - Program Protection for Practitioners

Course Learning/Performance Objectives followed by enabling learning objectives

ENG 260.U05.01.06	Given program protection acquisition lifecycle scenarios explain how protection measures are verified by T &E, DCMA and DSS.