



DEFENSE ACQUISITION UNIVERSITY

ACQ 160 Program Protection Planning Awareness

160718

Course Learning/Performance Objectives followed by its enabling learning objectives on separate lines if specified.

1	Recognize system security threats and consequences to acquisition programs and that the system security solution approach includes risk-based prevention, detection, and response to system security threats
	Define threats and attacks.
	Recognize the threat of critical program information (CPI) compromise and the threat of malicious insertion into software, hardware, and the supply chain.
	Match attacks to associated threats.
	Recognize examples of system and mission consequences of successful attacks associated with the threats of CPI compromise and the threats of malicious insertion.
	Identify the changes in the environment that are enabling threats of CPI compromise and threats of malicious insertion.
	Recognize the limitations of prevention measures to reduce risk.
	Determine how detection and response measures work in conjunction with prevention measures.
	Match examples of protection measures to the applicable category (prevention, detection, and response).
Recognize that protection measures influence system design and Statement of Work (SOW) tasks.	
2	Define critical program information (CPI), CPI policy, CPI threat definition, and associated attacks.
	Recognize the definition of critical program information.
	Recognize the critical program information that needs to be protected
	Recognize the policy that requires the identification and protection of critical program information.
3	Identify trusted system and network threat definitions, associated attacks, and policy.
	Recognize the definition of malicious insertion threat and the areas program protection seeks to protect against malicious insertion.
	Recognize attacks and consequences of malicious insertion threats.
	Recognize the policies that require the protection of critical functions and components.
4	Given DoDI 5000.02, recognize the requirement of the Program Protection Plan (PPP) within the Acquisition Life Cycle and how program protection is incorporated into the Request for Proposal (RFP).
	Recognize the program protection requirements specified by DoDI 5000.02.
	Recognize the purpose of program protection and the expected outcomes of implementing program protection processes.
	Recognize the required Program Protection Plan (PPP) approvals throughout the Acquisition Life Cycle.
	Recognize the content required in the PPP as specified by the PPP Outline and Guidance.
	Recognize sources of PPP guidance.
	Recognize the relationship between DoDI 5000.02 and other program protection policies.
Recognize the relationship between program protection and other acquisition activities (e.g., acquisition strategy, design for exportability, test and evaluation, systems engineering technical reviews, and cybersecurity).	
5	In accordance with DoDI 5000.02, define the roles and responsibilities of the program manager (PM), systems engineer (SE), system security engineer (SSE), system security engineering specialists, security specialists, chief developmental tester, and the contractor with respect to system security.
	Recognize the program protection roles and responsibilities of the program manager.
	Recognize the program protection roles and responsibilities of the systems engineer.
	Recognize the program protection roles and responsibilities of the system security engineer.
	Recognize the program protection roles and responsibilities of the system security engineering specialists.
	Recognize the program protection roles and responsibilities of the security specialists.
	Recognize the program protection roles and responsibilities of the chief developmental tester.
Recognize the program protection roles and responsibilities of the contractor.	
6	In accordance with DoDI 5000.02, recognize how program protection integrates system security engineering specialties and security specialties through a high level overview of each specialty's activities and outputs.
	Recognize the specialties that are considered part of program protection and how these specialties are integrated through program protection.
	Recognize the anti-tamper policy requirements, relationship to program protection, relationship to system design, and relationship to acquisition.
	Recognize the cybersecurity policy requirements, relationship to program protection, relationship to system design, and relationship to acquisition.
	Recognize the Defense Exportability Features (DEF) policy requirements, relationship to program protection, relationship to system design, and relationship to acquisition.
	Recognize the hardware assurance policy requirements, relationship to program protection, relationship to system design, and relationship to acquisition.
	Recognize the software assurance policy requirements, relationship to program protection, relationship to system design, and relationship to acquisition.
	Recognize the supply chain risk management policy requirements, relationship to program protection, relationship to system design, and relationship to acquisition.
Recognize characteristics of security specialties and their influence on program protection planning.	



DEFENSE ACQUISITION UNIVERSITY

ACQ 160 Program Protection Planning Awareness

160718

Course Learning/Performance Objectives followed by its enabling learning objectives on separate lines if specified.

	Recognize how test and evaluation (T&E), verification, and validation are interrelated and integrated across all system security engineering (SSE) and security specialties.
7	Recognize elements of information analysis for security implementation.
	Recognize the definitions of classified information and controlled unclassified information (CUI).
	Recognize the importance of classified information and unclassified technical information.
	Recognize the types of classified information and CUI.
	Recognize the criteria for classifying information and identifying CUI.
	Recognize the policy that requires the classification of information.
	Recognize the purpose of the National Industrial Security Program Operating Manual (NISPOM) and its relationship to industry.
	Recognize the criteria and policy for identifying and marking technical information.
	Identify the application of the information security policies to program protection.
	Recognize the requirements of Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, and program manager (PM) responsibilities related to the clause.
	Recognize the relationship between protection of information and other system security engineering (SSE) analyses and security specialties.
	Match acquisition information analysis scenarios to the protection requirements and methods.
	Recognize the role of the Defense Security Service (DSS) as part of the National Industrial Security Program (NISP).
	Identify the reporting/information Defense Security Service (DSS) makes available.
Recognize where Defense Security Service (DSS) reports can inform acquisition and security decisions.	
8	Recognize the elements of Critical Protection Information (CPI) analysis for security implementation.
	Recognize the process for identifying critical program information (CPI) and the outcomes of this process.
	Recognize key factors for assessing the risk to critical program information (CPI) and the outcome of this assessment.
	Identify the system security engineering specialties that are applicable to critical program information (CPI) protection measures.
	Recognize the horizontal protection process and its associated benefits.
	Identify the impacts of critical program information (CPI) identification and protection on the Program Protection Plan (PPP), the system design, and the acquisition.
Recognize appropriate critical program information (CPI) identification and protection activities across the Acquisition Life Cycle.	
9	Recognize elements of trusted systems and networks (TSN) analysis for security implementation.
	Recognize the criticality analysis process and its outcomes.
	Recognize the threat assessment process and its outcomes.
	Recognize vulnerability assessment intent, characteristics, and activities.
	Recognize the process for assessing the risk to trusted systems and networks (TSN) and its outcomes.
	Define at a top level the trusted systems and networks (TSN) protection measures trade-off analysis, including its goals and outcomes.
	Identify the system security engineering (SSE) specialties and security specialties that are applicable to trusted systems and networks (TSN) protection measures.
	Match acquisition scenarios to expected trusted systems and networks (TSN) protection actions.
Identify the impacts of trusted systems and networks (TSN) analysis on the PPP, the system design, and the acquisition.	
10	Recognize the purpose and characteristics of trade-off analysis and how program protection requirements are incorporated into the Request for Proposal.
	Recognize the purpose of trade-off analysis with system security engineering, systems engineering, performance, cost, and risk.
	Recognize characteristics of systems engineering trade-off analysis
	Recognize characteristics of system security engineering trade-off analysis.
	Recognize the factors considered in system security engineering (SSE) (including security specialties) for trade-off analysis.
	Define the sections of the Request for Proposal (RFP) that are affected by program protection.
	Recognize how program protection activities, protection measures, and mitigations are incorporated into the affected sections of the Request for Proposal (RFP) (Section C (SOW and SRD), I, J, L, M, and Exhibit A (CDRI)).
	Define how the National Industrial Security Program Operating Manual (NISPOM) activities are incorporated into the Request for Proposal (RFP) (e.g., DD 254).
	Define how Defense Federal Acquisition Regulation Supplement (DFARS) clauses are included in the Request for Proposal (RFP).
11	Recognize the role of test and evaluation for verification and validation of program protection measures.
	Define the relationship between the TEMP and the Program Protection Plan (PPP).
	Provide an overview, from the perspective of program protection, of the TEMP and the Developmental Evaluation Framework included in the TEMP, and their relationship to program protection.
	Define how system security engineering (SSE) specialties are incorporated into the Developmental Evaluation Framework included in the TEMP.



DEFENSE ACQUISITION UNIVERSITY
ACQ 160 Program Protection Planning Awareness

160718

*Course Learning/Performance Objectives followed by its
enabling learning objectives on separate lines if specified.*

	Recognize SSE and T&E interactions, support, and coordination activities and responsibilities within the Acquisition Life Cycle.
12	Recognize the role of test and evaluation for verification and validation of program protection measures.
	Define the relationship between the Test and Evaluation Master Plan (TEMP) and the Program Protection Plan (PPP).
	Provide an overview, from the perspective of program protection, of the TEMP and the Developmental Evaluation Framework included in the TEMP, and their relationship to program protection.
	Define how system security engineering (SSE) specialties are incorporated into the Developmental Evaluation Framework included in the TEMP.
	Recognize SSE and T&E interactions, support, and coordination activities and responsibilities within the Acquisition Life Cycle.
	Define SSE and security specialties roles and responsibilities during the Operations and Support (O&S) Phase.
13	Given DoDI 5200.39 and 5200.44, recognize the impact of SSE analyses on the technical baselines and systems engineering technical reviews.
	Define expected SSE analysis, inputs, and products for the Materiel Solution Analysis (MSA) Phase.
	Define expected SSE analysis, inputs, and products for the Technology Maturation and Risk Reduction (TMRR) Phase.
	Define expected SSE analysis, inputs, and products for the Engineering and Manufacturing Development (EMD) Phase.
	Define expected SSE analysis, inputs, and products for the Production and Deployment (P&D) Phase.
	Define SSE and security specialties roles and responsibilities during the Operations and Support (O&S) Phase.
14	Given contracting scenarios, relate the protection measure and mitigation steps to specific acquisition solicitations scenarios.
	Recognize how program protection planning concepts, principles, and practices have been applied in a program that is currently in the Materiel Solution Analysis (MSA) Phase, preparing the Request for Proposal (RFP) to enter the Technology Maturation and Risk Reduction (TMRR) Phase of the Acquisition Life Cycle.
	Recognize how program protection planning concepts, principles, and practices have been applied in a program that is currently in the Technology Maturation and Risk Reduction (TMRR) Phase, preparing the Request for Proposal (RFP) to enter the Engineering and Manufacturing Development (EMD) Phase of the Acquisition Life Cycle.
	Recognize how program protection planning concepts, principles, and practices have been applied in a program that is currently in the Engineering and Manufacturing Development (EMD) Phase, preparing the Request for Proposal (RFP) to enter the Production and Deployment (P&D) Phase of the Acquisition Life Cycle.
	Recognize how program protection planning concepts, principles, and practices have been applied in a commercial-off-the-shelf (COTS) enterprise resource planning (ERP) program.