Objectives Sheet

ACQ 160 - Program Protection Planning Awareness

Course Learning/Performance Objectives followed by enabling learning objectives

ACQ 160.U01.01	**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**
ACQ 160.U01.01.01	Define threats and attacks.
ACQ 160.U01.01.02	Recognize the threat of critical program information (CPI) compromise and the threat of malicious insertion into software, hardware, and the supply chain.
ACQ 160.U01.01.03	Match attacks to associated threats.
ACQ 160.U01.01.04	Recognize examples of system and mission consequences of successful attacks associated with the threats of CPI compromise and the threats of malicious insertion.
ACQ 160.U01.01.05	Identify the changes in the environment that are enabling threats of CPI compromise and threats of malicious insertion.
ACQ 160.U01.01.06	Recognize the limitations of prevention measures to reduce risk.
ACQ 160.U01.01.07	Determine how detection and response measures work in conjunction with prevention measures.
ACQ 160.U01.01.08	Match examples of protection measures to the applicable category (prevention, detection, and response).
ACQ 160.U01.01.09	Recognize that protection measures influence system design and Statement of Work (SOW) tasks.
ACQ 160.U02.01	**Define critical program information (CPI), CPI policy, CPI threat definition, and associated attacks.**
ACQ 160.U02.01.01	Recognize the definition of critical program information.
ACQ 160.U02.01.02	Recognize the critical program information that needs to be protected
ACQ 160.U02.01.03	Recognize the policy that requires the identification and protection of critical program information.
ACQ 160.U02.01.04	Recognize the consequences of compromised critical program information.
ACQ 160.U02.02	**Identify trusted system and network threat definitions, associated attacks, and policy.**
ACQ 160.U02.02.01	Recognize the definition of malicious insertion threat and the areas program protection seeks to protect against malicious insertion.
ACQ 160.U02.02.02	Recognize attacks and consequences of malicious insertion threats.
ACQ 160.U02.02.03	Recognize the policies that require the protection of critical functions and components.
ACQ 160.U02.02.04	Recognize the critical functions and components that need to be protected.
ACQ 160.U03.01	**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).**
ACQ 160.U03.01.01	Recognize the program protection requirements specified by DoDI 5000.02.
ACQ 160.U03.01.02	Recognize the purpose of program protection and the expected outcomes of implementing program protection processes.
ACQ 160.U03.01.03	Recognize the required Program Protection Plan (PPP) approvals throughout the Acquisition Life Cycle.
ACQ 160.U03.01.04	Recognize the content required in the PPP as specified by the PPP Outline and Guidance.
ACQ 160.U03.01.05	Recognize sources of PPP guidance.
ACQ 160.U03.01.06	Recognize the relationship between DoDI 5000.02 and other program protection policies.
ACQ 160.U03.01.07	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).
ACQ 160.U04.01	**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.**
ACQ 160.U04.01.01	Recognize the program protection roles and responsibilities of the program manager.
ACQ 160.U04.01.02	Recognize the program protection roles and responsibilities of the systems engineer.
ACQ 160.U04.01.03	Recognize the program protection roles and responsibilities of the system security engineer.
ACQ 160.U04.01.04	Recognize the program protection roles and responsibilities of the system security engineering specialists.
ACQ 160.U04.01.05	Recognize the program protection roles and responsibilities of the security specialists.
ACQ 160.U04.01.06	Recognize the program protection roles and responsibilities of the chief developmental tester.
ACQ 160.U04.01.07	Recognize the program protection roles and responsibilities of the contractor.
ACQ 160.U05.01	**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.**
ACQ 160.U05.01.01	Recognize the specialties that are considered part of program protection and how these specialties are integrated through program protection.
ACQ 160.U05.01.02	Recognize the anti-tamper policy requirements, relationship to program protection, relationship to system design, and relationship to acquisition.
ACQ 160.U05.01.03	Recognize the cybersecurity policy requirements, relationship to program protection, relationship to system design, and relationship to acquisition.

Objectives Sheet

ACQ 160 - Program Protection Planning Awareness

Course Learning/Performance Objectives followed by enabling learning objectives

ACQ 160.U05.01.04	Recognize the Defense Exportability Features (DEF) policy requirements, relationship to program protection, relationship to system design, and relationship to acquisition.
ACQ 160.U05.01.05	Recognize the hardware assurance policy requirements, relationship to program protection, relationship to system design, and relationship to acquisition.
ACQ 160.U05.01.06	Recognize the software assurance policy requirements, relationship to program protection, relationship to system design, and relationship to acquisition.
ACQ 160.U05.01.07	Recognize the supply chain risk management policy requirements, relationship to program protection, relationship to system design, and relationship to acquisition.
ACQ 160.U05.01.08	Recognize characteristics of security specialties and their influence on program protection planning.
ACQ 160.U05.01.09	Recognize how test and evaluation (T&E), verification, and validation are interrelated and integrated across all system security engineering (SSE) and security specialties.
ACQ 160.U06.01	**Recognize elements of information analysis for security implementation.**
ACQ 160.U06.01.01	Recognize the definitions of classified information and controlled unclassified information (CUI).
ACQ 160.U06.01.02	Recognize the importance of classified information and unclassified technical information.
ACQ 160.U06.01.03	Recognize the types of classified information and CUI.
ACQ 160.U06.01.04	Recognize the criteria for classifying information and identifying CUI.
ACQ 160.U06.01.05	Recognize the policy that requires the classification of information.
ACQ 160.U06.01.06	Recognize the purpose of the National Industrial Security Program Operating Manual (NISPOM) and its relationship to industry.
ACQ 160.U06.01.07	Recognize the criteria and policy for identifying and marking technical information.
ACQ 160.U06.01.08	Identify the application of the information security policies to program protection.
ACQ 160.U06.01.09	Recognize the requirements of Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, and program manager (PM) responsibilities related to the clause.
ACQ 160.U06.01.10	Recognize the relationship between protection of information and other system security engineering (SSE) analyses and security specialties.
ACQ 160.U06.01.11	Match acquisition information analysis scenarios to the protection requirements and methods.
ACQ 160.U06.01.12	Recognize the role of the Defense Security Service (DSS) as part of the National Industrial Security Program (NISP).
ACQ 160.U06.01.13	Identify the reporting/information Defense Security Service (DSS) makes available.
ACQ 160.U06.01.14	Recognize where Defense Security Service (DSS) reports can inform acquisition and security decisions.
ACQ 160.U07.01	**Recognize the elements of Critical Protection Information (CPI) analysis for security implementation.**
ACQ 160.U07.01.01	Recognize the process for identifying critical program information (CPI) and the outcomes of this process.
ACQ 160.U07.01.02	Recognize key factors for assessing the risk to critical program information (CPI) and the outcome of this assessment.
ACQ 160.U07.01.03	Identify the system security engineering specialties that are applicable to critical program information (CPI) protection measures.
ACQ 160.U07.01.04	Recognize the horizontal protection process and its associated benefits.
ACQ 160.U07.01.05	Identify the impacts of critical program information (CPI) identification and protection on the Program Protection Plan (PPP), the system design, and the acquisition.
ACQ 160.U07.01.06	Recognize appropriate critical program information (CPI) identification and protection activities across the Acquisition Life Cycle.
ACQ 160.U08.01	**Recognize elements of trusted systems and networks (TSN) analysis for security implementation.**
ACQ 160.U08.01.01	Recognize the criticality analysis process and its outcomes.
ACQ 160.U08.01.02	Recognize the threat assessment process and its outcomes.
ACQ 160.U08.01.03	Recognize vulnerability assessment intent, characteristics, and activities.
ACQ 160.U08.01.04	Recognize the process for assessing the risk to trusted systems and networks (TSN) and its outcomes.
ACQ 160.U08.01.05	Define at a top level the trusted systems and networks (TSN) protection measures trade- off analysis, including its goals and outcomes.
ACQ 160.U08.01.06	Identify the system security engineering (SSE) specialties and security specialties that are applicable to trusted systems and networks (TSN) protection measures.
ACQ 160.U08.01.07	Match acquisition scenarios to expected trusted systems and networks (TSN) protection actions.
ACQ 160.U08.01.08	Identify the impacts of trusted systems and networks (TSN) analysis on the PPP, the system design, and the acquisition.
ACQ 160.U09.01	**Recognize the purpose and characteristics of trade-off analysis and how program protection requirements are incorporated into the Request for Proposal.**
ACQ 160.U09.01.01	Recognize the purpose of trade-off analysis with system security engineering, systems engineering, performance, cost, and risk.

Objectives Sheet

ACQ 160 - Program Protection Planning Awareness

Course Learning/Performance Objectives followed by enabling learning objectives

ACQ 160.U09.01.02	Recognize characteristics of systems engineering trade-off analysis
ACQ 160.U09.01.03	Recognize characteristics of system security engineering trade-off analysis.
ACQ 160.U09.01.04	Recognize the factors considered in system security engineering (SSE) (including security specialties) for trade- off analysis.
ACQ 160.U09.01.05	Define the sections of the Request for Proposal (RFP) that are affected by program protection.
ACQ 160.U09.01.06	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 (CDRL)).
ACQ 160.U09.01.07	Define how the National Industrial Security Program Operating Manual (NISPOM) activities are incorporated into the Request for Proposal (RFP) (e.g., DD 254).
ACQ 160.U09.01.08	Define how Defense Federal Acquisition Regulation Supplement (DFARS) clauses are included in the Request for Proposal (RFP).
ACQ 160.U10.01	**Recognize the role of test and evaluation for verification and validation of program protection measures.**
ACQ 160.U10.01.01	Define the relationship between the TEMP and the Program Protection Plan (PPP).
ACQ 160.U10.01.02	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.
ACQ 160.U10.01.03	Define how system security engineering (SSE) specialties are incorporated into the Developmental Evaluation Framework included in the TEMP.
ACQ 160.U10.01.04	Recognize SSE and T&E interactions, support, and coordination activities and responsibilities within the Acquisition Life Cycle.
ACQ 160.U10.02	**Recognize the role of test and evaluation for verification and validation of program protection measures.**
ACQ 160.U10.02.01	Define the relationship between the Test and Evaluation Master Plan (TEMP) and the Program Protection Plan (PPP).
ACQ 160.U10.02.02	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.
ACQ 160.U10.02.03	Define how system security engineering (SSE) specialties are incorporated into the Developmental Evaluation Framework included in the TEMP.
ACQ 160.U10.02.04	Recognize SSE and T&E interactions, support, and coordination activities and responsibilities within the Acquisition Life Cycle.
ACQ 160.U10.02.05	Define SSE and security specialties roles and responsibilities during the Operations and Support (O&S) Phase.
ACQ 160.U10.03	**Given DoDI 5200.39 and 5200.44, recognize the impact of SSE analyses on the technical baselines and systems engineering technical reviews.**
ACQ 160.U10.03.01	Define expected SSE analysis, inputs, and products for the Materiel Solution Analysis (MSA) Phase.
ACQ 160.U10.03.02	Define expected SSE analysis, inputs, and products for the Technology Maturation and Risk Reduction (TMRR) Phase.
ACQ 160.U10.03.03	Define expected SSE analysis, inputs, and products for the Engineering and Manufacturing Development (EMD) Phase.
ACQ 160.U10.03.04	Define expected SSE analysis, inputs, and products for the Production and Deployment (P&D) Phase.
ACQ 160.U10.03.05	Define SSE and security specialties roles and responsibilities during the Operations and Support (O&S) Phase.
ACQ 160.U11.01	**Given contracting scenarios, relate the protection measure and mitigation steps to specific acquisition solicitations scenarios.**
ACQ 160.U11.01.01	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.
ACQ 160.U11.01.02	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.
ACQ 160.U11.01.03	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.
ACQ 160.U11.01.04	Recognize how program protection planning concepts, principles, and practices have been applied in a commercial-off-the-shelf (COTS) enterprise resource planning (ERP) program.