

Student Guide

Acquisitions and Contracting Basics in the National Industrial Security Program (NISP)

Lesson 1: Course Introduction

Contents

Introduction	2
Opening.....	2
Objectives.....	2

Introduction

Opening

Weapon System Project Manager: Welcome, everyone. The weapon system on the screen, comprising new critical technology, has passed testing successfully and is in production. We now have identified the need for a smaller scale weapon system for launch and recovery to smaller ships as well as to perform land-based missions.

Security Specialist: The sophistication of this new weapon system means there will be a number of subcontractor companies working with a prime contractor to contribute to the design and development of the assemblies and components. Given how many suppliers will be needed for a single subsystem, we'll need to manage risk in the contracts and collaborate with System Security Engineers to ensure countermeasures are designed-in and vulnerabilities are engineered-out.

Information System Security Specialist (ISSP): We're also going to have to be vigilant to ensure we have the right requirements in place to mitigate threats and vulnerabilities to the information and communications technology, or ICT.

Counterintelligence: You can bet that our adversaries are going to be probing for entryways to get their hands on these design specifications, not to mention the supply chain providers further down the road on this program.

Narrator: Do you know how and when to plan for security throughout the acquisition life cycle? When should your role begin? When are security requirements defined?

Welcome to the Acquisitions and Contracting Basics in the National Industrial Security Program (NISP) course.

Objectives

This course will provide an overview of the Department of Defense (DoD) acquisition life cycle and the role of security professionals. It will also provide an overview of the contracting process and how security professionals support it from requirements definition in the pre-systems acquisition stage through sustainment.

Here are the course objectives:

- Identify the phases in the acquisition life cycle
- Identify the role of security professionals in the DoD acquisition life cycle
- Identify the importance of planning for security across the acquisition life cycle and during the contracting process
- Identify the phases of contract administration and the impact of security requirements in the contracting process

- Identify the purpose of the security related contractual documents: DD Form 254, DD Form 441, and SF 328
- Identify the relationship of the Statement of Work (SOW) and Performance Work Statement (PWS) to DD Form 254

Student Guide

Acquisitions and Contracting Basics in the National Industrial Security Program (NISP)

Lesson 2: DoD Acquisition Life Cycle and Security Requirements

Contents

Introduction	3
Objectives.....	3
National Industrial Security Program and the DoD Acquisition Life Cycle	3
The National Industrial Security Program.....	3
DoD Acquisition Life Cycle.....	4
DoD Acquisition Life Cycle Milestones.....	4
Milestones and Decision Points	5
Acquisition Management and Security	9
Government and Contractor Roles	10
Roles and Responsibilities for Security Requirements.....	11
What is a Classified Contract?	11
Contracting Officer and the COR	12
Defense Security Service (DSS).....	12
Contractor Responsibilities	12
NISP Contract Classification System (NCCS).....	13
Review Activities	14
Review Activity 1	14
Review Activity 2	15
Review Activity 3	16
Conclusion	17

Lesson Summary.....	17
Answer Key.....	18
Review Activity 1	18
Review Activity 2	19
Review Activity 3	20

Introduction

Objectives

As security professionals, you ensure our nation's weapon systems, classified and sensitive information and communications technology do not fall into the hands of our adversaries.

You play an important role in preventing access to data and thwarting acts of espionage, sabotage, and theft.

Understanding the role of security in the context of the five phases of the DoD acquisition life cycle, from requirements definition through sustainment, will help keep our nation's secrets out of the hands of our adversaries.

Here are the lesson objectives:

- Identify the phases in the acquisition life cycle
 - Identify the important role of the National Industrial Security Program (NISP) in the acquisition life cycle
 - Identify the process for moving an acquisition through the life cycle phases
- Identify the role of security professionals in the DoD contracting process
 - Identify the key government roles and responsibilities in the DoD acquisition life cycle
 - Identify the key contractor roles and responsibilities in the DoD acquisition life cycle

National Industrial Security Program and the DoD Acquisition Life Cycle

The National Industrial Security Program

U.S. industry develops and produces the majority of our nation's technology, much of which is classified.

The National Industrial Security Program (NISP) was established to ensure that cleared industry safeguards classified information in their possession, or which they access, while performing work on contracts, programs, bids, and/or research and development efforts. The NISP is a partnership between the federal government and private industry to safeguard classified information. It applies to all Executive Branch Departments and Agencies and contractors within the U.S. and its territories.

The National Industrial Security Program Operating Manual (NISPOM) defines the requirements, restrictions, and safeguards that industry must follow. These protections are in place before any classified work may begin. Government agencies have the responsibility to provide security requirements for all requests for proposals and contracts that require access to classified information.

DoD Acquisition Life Cycle

The Department of Defense Instruction (DoDI), 5000.02 provides guidance on the Operation of the Defense Acquisition System. The emphasis in this updated instruction is on tailoring procedures and processes for the individual program's needs. It presents DoD acquisition life cycle models with different entry points, depending on the type of service or product being acquired or the need for accelerated acquisition. This lesson will focus on a generic acquisition process.

The acquisition process begins when a need is identified for a service or product in support of the Warfighter. An initial requirements document, such as the Initial Capabilities Document (ICD), is examined and validated and a plan is framed for undertaking the Analysis of Alternatives (AoA).

Once this work is completed the Materiel Development Decision is made that a new product is needed and that activities to analyze alternative solutions will occur. The decision effectively directs execution of the AoA and authorizes the DoD Component to conduct the Materiel Solution Analysis Phase. This decision point is the entry point into the acquisition process for all defense acquisition products.

There are five phases in the acquisition life cycle. Materiel Solution Analysis is Phase 1 and Technology Maturation and Risk Reduction (TMRR) is Phase 2. Together these two phases constitute the Pre-System Acquisition process of the Defense Acquisition Management System. Phase 3, Engineering and Manufacturing Development (EMD) and Phase 4, Production and Deployment, or P&D, constitute the System Acquisition process. Phase 5 is Operations and Support (O&S) which is the sustainment part of the process.

DoD Acquisition Life Cycle Milestones

The purpose of milestone decision reviews embedded in the acquisition process is to assess a program's readiness to proceed to the next acquisition phase. In order to advance to the next phase, the program must meet the exit criteria required at each milestone, including successful supportability design reviews.

Technical design reviews and tests throughout the acquisitions process confirm traceable requirements flow down to ensure an effective, supportable, affordable system. For more detailed information on the technical reviews, consult the Defense Acquisition Guidebook, Chapter 4, Systems Engineering.

Milestone decision reviews ensure that a sound investment decision committing the Department's financial resources is made.

Milestones and Decision Points

Milestone A approval is a risk reduction decision. It is an investment decision to pursue specific product or design concepts and to commit the necessary resources. These resources are required to mature technology and/or reduce risks that must be mitigated prior to a decision committing the resources needed for development.

For new weapon systems or services, a contract may be executed in TMRR for engineering design and supportability analysis, also called product support analysis. There are two major decision points to advance the program during TMRR.

The Capability Design Document (CDD) validation is a requirements decision point. CDD approval means that major cost and performance trades have been completed and enough risk reduction has been completed to support a decision to commit to the set of requirements. In turn, these requirements are used for preliminary design activities, development, and production.

The Development RFP Release Decision is the point at which planning for development is complete and a decision is made to release a Request for Proposal (RFP). The RFP for development (and possibly initial production) is released to industry.

An "acquisition program" is not formally initiated (with the accompanying statutory requirements) until Milestone B, or at Milestone C for those programs that enter directly at Milestone C.

Milestone B approval is a development decision that commits resources. It authorizes proceeding to award of the contract or contracts needed to conduct development leading to production and field of the product.

Milestone C is the initial production decision, also known as Low-Rate Initial Production (LRIP) as well as Limited Deployment for software systems. Milestone C exit criteria are dependent on an approved Capability Production Document (CPD). It is usually based on developmental test results that ensure the product meets form, fit, and function in the appropriate environment with no significant manufacturing risks. This milestone approval commits the resources and authorizes awarding the contract or contracts required to enter production and begin fielding the product or service. The commitment to enter production is very difficult and expensive to reverse.

During the Production and Deployment (P&D) Phase, the decision to enter into Full Rate Production is approved. Phase 5, Operations and Support, begins the sustainment period for the fielded product.

Review each phase of the Acquisition Life Cycle below to learn more about the activities that are essential to milestone decision approvals.

Phase 1: Materiel Solution Analysis

The purpose of the Materiel Solution Analysis phase is to conduct the analysis and other activities needed to choose the concept for the product that will be acquired.

During Materiel Solution Analysis, the following activities occur:

- Conduct analysis and other activities needed to choose the concept for the product that will be acquired.
- Begin translating validated capability gaps into system-specific requirements including the Key Performance Parameters (KPPs), Key System Attributes (KSAs).
- Conduct planning to support a decision on the acquisition strategy for the product.
- Analysis of Alternative (AoA) solutions, key trades between cost and performance, affordability analysis, risk analysis, and planning for risk mitigation are key activities in this phase.
- Component Acquisition Executive selects a Program Manager and establishes a program office to plan the acquisition program with emphasis on the next phase.

Phase 2: Technology Maturation & Risk Reduction (TMRR)

The purpose of the TMRR phase is to reduce technology, engineering, integration, and life-cycle cost risk to the point that a decision to contract for EMD can be made with confidence in successful program execution for development, production, and sustainment.

During TMRR, the following activities occur:

- Includes a mix of activities intended to reduce specific risks associated with the product to be developed.
- Additional design trades and requirements trades necessary to ensure an affordable product and executable development and production programs are made.
- Normally includes competitive sources conducting technology maturation and risk reduction activities and preliminary design activities up to and

including Preliminary Design Review (PDR) prior to source selection for the Engineering and Manufacturing Development (EMD) phase.

Phase 3: Engineering and Manufacturing Development (EMD)

The purpose of the EMD activities is to achieve Initial Operational Capability (IOC) and to demonstrate an affordable, supportable, interoperable, and producible system in its intended environment.

The CDD, Acquisition Strategy, System Engineering Plan, and Test and Evaluation Master Plan guide the EMD effort.

During EMD, the following activities occur:

- Develop a system or an increment of capability
- Complete full system integration
- Develop an affordable and executable manufacturing process
- Ensure operational supportability with particular attention to minimizing the logistics footprint
- Implement human systems integration (HSI)
- Design for reducibility
- Ensure affordability
- Protect Critical Program Information (CPI) by implementing appropriate techniques such as anti-tamper
- Demonstrate system integration, interoperability, safety, and utility.

Phase 4: Production and Deployment (P&D)

The purpose of the Production and Deployment phase is to achieve Full Operational Capability (FOC) that satisfies mission needs.

In making the Full-Rate Production Decision or the Full Deployment Decision, the MDA will consider any new validated threat environments that might affect operational effectiveness, and may consult with the requirements validation authority as part of the decision making process to ensure that capability requirements are current.

During Production and Deployment, the following activities occur:

- Remaining production or deployment of the product is completed, (e.g., LRIP, Limited Deployment, OT&E, and the Full-Rate Production Decision

or the Full Deployment Decision) leading to Full Operational Capability (FOC).

- Except as specifically approved by the Milestone Decision Authority (MDA) critical deficiencies identified in testing will be resolved prior to proceeding beyond LRIP or Limited Deployment.
- The Operational organization has been equipped and trained and is determined to be capable of conducting mission operations.
- All system sustainment and support activities are initiated, if they have not already commenced.
- Should Cost management and other techniques will be used continuously to control and reduce cost.

Phase 5: Operations and Support (O&S)

The O&S Phase begins after the production or deployment decision and is based on an MDA-approved Life Cycle Sustainment Plan (LCSP).

The purpose of the O&S Phase is to execute the product support strategy, satisfy materiel readiness and operational support performance requirements, and sustain the system over its life cycle (to include disposal).

There are two major efforts during O&S, Sustainment and Disposal. The LCSP is the basis for the activities in this phase.

During O&S, the following activities occur:

- Execute the product support strategy.
- Satisfy materiel readiness and operational support performance requirements.
- Sustain the system over its life cycle.

Sustainment

- Deploy the product support package and monitor its performance according to the LCSP
- Program Manager
 - Ensures resources are programmed and necessary IP deliverables and associated license rights, tools, equipment, and facilities are acquired to support each of the levels of maintenance that will provide product support; and

- Establishes necessary organic depot maintenance capability in compliance with statute and the LCSP.

Disposal

- At the end of its useful life, a system will be demilitarized and disposed of in accordance with all legal and regulatory requirements and policy relating to safety (including explosives safety), security, and the environment.

Acquisition Management and Security

Government security offices are integrated throughout the program and acquisition life cycle when the acquisition effort involves classified access. Security personnel should begin to work on a program as soon as the decision is made to begin the Materiel Solution Analysis Phase, research and development (R&D) or Request for Proposal discussions. Security personnel collaborate with the program and contracting personnel to frame the requirements, restrictions, and other safeguards to protect classified information.

Recall that as milestones are achieved, new contracts may be issued through the acquisition life cycle. Security requirements are revisited with each new contract. When security requirements such as these exist, they must be included in a DD Form 254 for every classified solicitation and contract.

The NISPOM ensures the uniform implementation of security requirements for the protection of classified information in the possession or accessed by industry.

NISPOM

NISPOM topics include:

- General policies and procedures
- Reporting requirements
- Facility clearances (FCLs)
- Personnel security clearances (PCLs)
- Foreign Ownership, Control, or Influence (FOCI) issues
- Security training and briefings
- Classification
- Marking requirements

- Safeguarding of classified information
- Visits and meetings
- Subcontracting
- Information System (IS) security
- Special requirements, including nuclear-related information, Critical Nuclear Weapon Design Information (CNWDI), intelligence information, and communications security (COMSEC)
- International security requirements

For more information on the NISP, see *Industrial Security Basics*, available through CDSE's Security, Training, Education and Professionalization Portal (STEPP).

DD Form 254 Contract Security Classification Specification

The Contract Security Classification Specification is mandatory and is updated through the life of the contract. It is designed to provide a contractor with the security requirements and classification guidance needed for performance on a contract that requires classified information.

The DD Form 254:

- Provides the contractor with specific clearance and access requirements
- Identifies a requirement to generate and store classified information at a contractor facility when required for contract performance
- Classification guidance
- Advises contractor on handling procedures for classified material received or generated

You will learn more about DD Form 254 in Lesson 4.

Government and Contractor Roles

Cognizant Security Agencies (CSAs) establish and oversee industrial security programs and administer security requirements. There are five CSAs that are ultimately responsible for the security of all cleared U.S. contractors. These agencies establish industrial security requirements, provide security guidance, advice, and assist contractors with industrial security. The CSAs also inspect and monitor cleared companies and determine eligibility for access to classified information.

The Government Contracting Activity (GCA) also plays a key role in protecting classified information entrusted to industry. The GCA has broad authority regarding acquisition functions for its agency, as delegated by the agency head. In addition to issuing the contract, the GCA ensures that contracts for classified work include the Federal Acquisition Regulation (FAR) Security Requirements clauses. The FAR System governs the "acquisition process" by which the federal government purchases (acquires) goods and services. The purpose of the FAR is to provide "uniform policies and procedures for acquisition."

The GCA also provides industry contractors with contract-specific guidance and oversight, including on the DoD Contract Security Classification Specification, or DD Form 254, for contracts requiring access to classified information and security classification and declassification guidance to contractors. The GCA handles other responsibilities as well. It sponsors facilities for a facility clearance, or FCL, and influences potential Foreign Ownership, Control, or Influence (FOCI) issues related to an FCL. You can find further information on the FCL and FOCI pages in the FSO toolkit located on the CDSE website. The GCA ensures the Original Classification Authority (OCA) conducts damage assessments in cases of loss, compromise, or suspected compromise of classified information.

Finally, on the industry side, contractors have the major responsibility to implement the NISP requirements to protect classified information.

Roles and Responsibilities for Security Requirements

What is a Classified Contract?

As you recall, most of our nation's technology is developed and produced by U.S. industry, and much of that technology is classified. Recall that the acquisition life cycle for a weapon system necessitates issuing multiple contracts as the program progresses through the phases.

The contracting process supports this progression and relies upon leadership from the Government Contracting Officer, the Contracting Officer's Representative, DSS, the GCA, and the contractor to protect classified information. You will learn about the contracting process in Lesson 4.

A "classified contract" is one that requires the contractor or one of the contractor's employees to have access to classified information to perform on the contract for services or products. Access to classified information can occur at the contractor facility, at a government facility or at another cleared contractor facility. Every classified contract issued to a contractor requires that the DoD Contract Security Classification Specification, DD Form 254, be included in the contract.

Contracting Officer and the COR

The Contracting Officer has a key role across the DoD acquisition life cycle with the authority to enter into, administer, and terminate contracts. The Contracting Officer is instrumental during the Pre-solicitation phase, Solicitation phase, and Award phase in the acquisition contracting process. Contracting Officers ensure the insertion of the Security Requirements clause. The Contracting Officer ensures all contract actions comply with appropriate laws, executive orders, regulations, and other applicable procedures and approvals.

The Contracting Officer's Representative (COR) is appointed by the Contracting Officer for a specific contract. The COR monitors performance on the contract, making sure that all of the necessary requirements are being met for the Contracting Officer as stipulated in the Performance Work Statement or Statement of Work.

The COR assures the contractor maintains an FCL and PCL's when access to classified information is required. CORs communicate the security requirements during the procurement process and contract performance.

Defense Security Service (DSS)

DSS serves as the Cognizant Security Office (CSO) for the DoD. As part of the organization with security oversight responsibility, DSS employees have a range of key responsibilities in implementing the NISP. DSS administers the NISP and provides guidance to and oversight of the over 13,000 contractor facilities cleared for access to classified information.

DSS is involved during all phases of the acquisition process if and only if there is a requirement for access to classified information and a company has an FCL. It grants FCLs and monitors facilities for changed conditions. DSS conducts security vulnerability assessments and other oversight activities to ensure protection of classified information. It also provides Industrial Security training and assigns an IS Rep to each contractor facility.

DSS works closely with the DoD Security Specialists, the GCA representatives to the NISP. DoD Security Specialists serve as security experts, and maintain security cognizance over all activity information, personnel, information systems, physical security and – most importantly for the NISP – industrial security.

Contractor Responsibilities

DD Form 441, DoD Security Agreement, is a security agreement between the US Government and the defense contractor. It documents each party's responsibilities for protecting classified information.

Contractors are responsible for executing and ensuring compliance with the agreement. They must also use the DD Form 254, Contract Security Classification Specification to establish a security program consistent with the security requirements of the contract. Each contract issued for classified work includes the DD Form 254. Prime contractors are responsible for issuing their subcontractors a subcontract with the DD Form 254.

The contractor ensures company employees comply with the NISP, following guidelines for monitoring approved classified information systems and other safeguarding measures defined in the National Industrial Security Program Operating Manual (NISPOM). The Facility Security Officer (FSO) works closely with the DSS Industrial Security Representative to maintain a viable security program.

The contractor is responsible for performing on the classified contract according to the Statement of Work (SOW) or Performance Work Statement (PWS).

The prime contractor is responsible for disclosing classified information to cleared subcontractors.

NISP Contract Classification System (NCCS)

The NISP Contract Classification System (NCCS) is an Enterprise Federal information system application that supports DoD and other Federal Agencies in the NISP. It facilitates the processing and distribution of Contract Security Classification Specifications, DD Form 254, for contracts requiring access to classified information.

NCCS provides a secure mechanism for creating and routing a DD Form 254 electronic equivalent to and from the respective security offices/organizations of both the government and the prospective vendor. The repository alleviates issues of timeliness, accuracy, duplication and more.

The NCCS automates the DD Form 254 and its processes and workflows.

Review Activities

Review Activity 1

For each statement, select the best response. Check your answers in the Answer Key at the end of this Student Guide.

Question 1 of 5

During this phase, the Capability Design Document approval decision is made, the Development Request for Proposal is released, and design and product support analysis is started.

- Materiel Solution Analysis (MSA) Phase
- Technology Maturation & Risk Reduction (TMRR) Phase
- Engineering & Manufacturing Development (EMD) Phase
- Production & Deployment (P&D) Phase
- Operations & Support (O&S) Phase

Question 2 of 5

During this phase, the activities focus on achieving Full Operational Capability that satisfies mission needs and ensures any new threat environments are considered.

- Materiel Solution Analysis (MSA) Phase
- Technology Maturation & Risk Reduction (TMRR) Phase
- Engineering & Manufacturing Development (EMD) Phase
- Production & Deployment (P&D) Phase Operations & Support (O&S) Phase

Question 3 of 5

During this phase, a new contract is awarded to demonstrate an affordable, supportable, interoperable, and producible system in its intended environment.

- Materiel Solution Analysis (MSA) Phase
- Technology Maturation & Risk Reduction (TMRR) Phase
- Engineering & Manufacturing Development (EMD) Phase
- Production & Deployment (P&D) Phase
- Operations & Support (O&S) Phase

Question 4 of 5

At the end of this phase, an investment decision is made based on an Analysis of Alternatives and other exit criteria to pursue specific product or design concepts and to commit the necessary resources.

- Materiel Solution Analysis (MSA) Phase
- Technology Maturation & Risk Reduction (TMRR) Phase
- Engineering & Manufacturing Development (EMD) Phase
- Production & Deployment (P&D) Phase
- Operations & Support (O&S) Phase

Question 5 of 5

During this phase, sustainment of the fielded product ensures associated license rights, tools, equipment, and facilities are acquired to support each of the levels of maintenance that will provide product support.

- Materiel Solution Analysis (MSA) Phase
- Technology Maturation & Risk Reduction (TMRR) Phase
- Engineering & Manufacturing Development (EMD) Phase
- Production & Deployment (P&D) Phase
- Operations & Support (O&S) Phase

Review Activity 2

Select True or False for each statement. Check your answers in the Answer Key at the end of this Student Guide.

Question 1 of 3

The Government Contracting Activity (GCA) ensures that contracts for classified work include the FAR Security Requirements and DD Form 254.

- True
- False

Question 2 of 3

The Cognizant Security Agencies (CSAs) inspect and monitor cleared companies and determines eligibility for access to classified information.

- True
- False

Question 3 of 3

Security personnel start work on a program as soon as the decision is made to begin the Engineering and Manufacturing Development Phase.

- True
- False

Review Activity 3

For each statement, select the best response. Check your answers in the Answer Key at the end of this Student Guide.

Question 1 of 4

Ensures the insertion of the FAR Security Requirements clause in the contract

- Contracting Officer's Representative (COR)
- Contracting Officer
- Defense Security Service (DSS)
- Contractor

Question 2 of 4

Issues subcontracts with the DD Form 254

- Contracting Officer's Representative (COR)
- Contracting Officer
- Defense Security Service (DSS)
- Contractor

Question 3 of 4

Monitors contract performance to ensure Performance Work Statement or Statement of Work requirements are met

- Contracting Officer's Representative (COR)
- Contracting Officer
- Defense Security Service (DSS)
- Contractor

Question 4 of 4

Conducts security vulnerability assessments on contractors and coordinates with the appropriate DoD representatives and Security Specialists on damage assessments.

- Contracting Officer's Representative (COR)
- Contracting Officer
- Defense Security Service (DSS)
- Contractor

Conclusion

Lesson Summary

You have completed the DoD Acquisition Life Cycle and Security Requirements lesson.

Answer Key

Review Activity 1

Question 1 of 5

During this phase, the Capability Design Document approval decision is made, the Development Request for Proposal is released, and design and product support analysis is started.

- Materiel Solution Analysis Phase
- Technology Maturation & Risk Reduction (TMRR) Phase (correct response)
- Engineering & Manufacturing Development (EMD) Phase
- Production & Deployment (P&D) Phase
- Operations & Support (O&S) Phase

Feedback: During the Technology Maturation & Risk Reduction Phase, the CDD is approved with system-specific requirements, the RFP is released to industry, and technical design and analyses begins.

Question 2 of 5

During this phase, the activities focus on achieving Full Operational Capability that satisfies mission needs and ensures any new threat environments are considered.

- Materiel Solution Analysis Phase
- Technology Maturation & Risk Reduction (TMRR) Phase
- Engineering & Manufacturing Development (EMD) Phase
- Production & Deployment (P&D) Phase (correct response)
- Operations & Support (O&S) Phase

Feedback: During the Production & Deployment Phase, activities focus on achieving Full Operational Capability and ensure any new threat environments are considered.

Question 3 of 5

During this phase, a new contract is awarded to demonstrate an affordable, supportable, interoperable, and producible system in its intended environment.

- Materiel Solution Analysis Phase
- Technology Maturation & Risk Reduction (TMRR) Phase
- Engineering & Manufacturing Development (EMD) Phase (correct response)
- Production & Deployment (P&D) Phase
- Operations & Support (O&S) Phase

Feedback: During the Engineering & Manufacturing Development Phase, a contract is awarded to demonstrate an affordable, supportable, interoperable, and producible system in its intended environment.

Question 4 of 5

At the end of this phase, an investment decision is made based on an Analysis of Alternatives and other exit criteria to pursue specific product or design concepts and to commit the necessary resources.

- Materiel Solution Analysis Phase (correct response)
- Technology Maturation & Risk Reduction (TMRR) Phase
- Engineering & Manufacturing Development (EMD) Phase
- Production & Deployment (P&D) Phase
- Operations & Support (O&S) Phase

Feedback: At the end of the Materiel Solution Analysis Phase an investment decision is made to pursue specific product or design concepts and to commit the necessary resources.

Question 5 of 5

During this phase, sustainment of the fielded product ensures associated license rights, tools, equipment, and facilities are acquired to support each of the levels of maintenance that will provide product support.

- Materiel Solution Analysis Phase
- Technology Maturation & Risk Reduction (TMRR) Phase
- Engineering & Manufacturing Development (EMD) Phase
- Production & Deployment (P&D) Phase
- Operations & Support (O&S) Phase (correct response)

Feedback: During the Operations & Support Phase concerns center on sustainment of the fielded system as well as disposal at end-of-life.

Review Activity 2

Question 1 of 3

The Government Contracting Activity (GCA) ensures that contracts for classified work include the FAR Security Requirements and DD Form 254.

- True (correct response)
- False

Feedback: The GCA ensures that contracts for classified work include the FAR Security Requirements and DD Form 254. The DoD Security Specialist is the GCA representative security expert.

Question 2 of 3

The Cognizant Security Agencies (CSAs) inspect and monitor cleared companies and determines eligibility for access to classified information.

- True (correct response)
- False

Feedback: The CSAs establish industrial security programs and provide security oversight to include monitoring cleared companies and determining eligibility for access to classified information.

Question 3 of 3

Security personnel start work on a program as soon as the decision is made to begin the Engineering and Manufacturing Development Phase.

- True
- False (correct response)

Feedback: Security personnel should begin work on a program as soon as the decision is made to begin the Material Solution Analysis Phase.

Review Activity 3

Question 1 of 4

Ensures the insertion of the FAR Security Requirements clause in the contract

- Contracting Officer's Representative (COR)
- Contracting Officer (correct response)
- Defense Security Service (DSS)
- Contractor

Feedback: The Contracting Officer ensures the insertion of the FAR Security Requirements clause in the contract.

Question 2 of 4

Issues subcontracts with the DD Form 254

- Contracting Officer's Representative (COR)
- Contracting Officer
- Defense Security Service (DSS)
- Contractor (correct response)

Feedback: The Prime Contractor issues subcontracts with the DD Form 254 to each of its subcontractors.

Question 3 of 4

Monitors contract performance to ensure Performance Work Statement or Statement of Work requirements are met

- Contracting Officer's Representative (COR) (correct response)
- Contracting Officer
- Defense Security Service (DSS)
- Contractor

Feedback: *The Contracting Officer's Representative monitors contract performance to ensure PWS or SOW requirements are met.*

Question 4 of 4

Conducts security vulnerability assessments on contractors and coordinates with the appropriate DoD representatives and Security Specialists on damage assessments.

- Contracting Officer's Representative (COR)
- Contracting Officer
- Defense Security Service (DSS) (correct response)
- Contractor

Feedback: *DSS conducts security vulnerability assessments and coordinates with the appropriate DoD representatives and Security Specialists on damage assessments in case of contractor loss, compromise, or suspected compromise of classified information.*

Student Guide

Acquisitions and Contracting Basics in the National Industrial Security Program (NISP)

Lesson 3: Security Requirements and Guidance

Contents

Introduction	3
Objectives.....	3
Security Requirements and Guidance in the FAR and NISPOM.....	3
FAR and the NISPOM	3
Security Requirements Clause.....	4
Classification Management.....	4
GCA Responsibilities	5
Contractor's Responsibilities.....	5
Security Requirements for Contractors.....	5
Contractors in Different Environments	5
Facility Clearance (FCL)	6
FCL Security Requirements.....	6
Contractor Security Requirements: Dos and Don'ts	7
Privity of Contract	7
Review Activities	9
Review Activity 1	9
Review Activity 2	9
Review Activity 3	10
Review Activity 4	10
Conclusion	11
Lesson Summary.....	11

Answer Key	12
Review Activity 1	12
Review Activity 2	13
Review Activity 3	13
Review Activity 4	14

Introduction

Objectives

In this lesson, you will delve into the policy and guidance that define the security requirements for classified contracts in the NISP. Then you will examine contractor security requirements.

Here are the lesson objectives:

- Identify the importance of planning for security across the acquisition life cycle and during the contracting process
 - Identify the relationship of contractual security requirements in the FAR and security guidance based on the NISPOM
 - Identify the responsibilities for security classification management
 - Identify security requirements for contractor participation in classified contracts
 - Distinguish between security requirements that can and cannot be required of the contractor

Security Requirements and Guidance in the FAR and NISPOM

FAR and the NISPOM

Contractual security requirements found in the FAR and security guidance based on the NISPOM and Component guidance derive from national level policy that establishes the National Industrial Security Program, or NISP, in Executive Order 12829. 32 CFR 2004, “NISP Implementing Directive,” of 2006, and its amendment in 2010, implement this executive order.

The Federal Acquisition Regulation, or FAR, provides uniform policies and procedures for acquisition and supports implementation of the requirements into contracts. Specifically, FAR Subpart 4.4, Safeguarding Classified Information Within Industry, addresses the incorporation of the requirements stated in Executive Order 12829, National Industrial Security Program. Subpart 4.4 states the following DoD publications implement the NISP including the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M and the Industrial Security Regulation (ISR), DoD 5220.22-R.

DoD guidance with respect to foreign ownership is outlined in DoD Manual 5220.22, Volume 3, “National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence, or FOCI” and Directive-type Memorandum (DTM) 15-002, “Policy Guidance for the Processing of National Interest Determinations, or NIDs in Connection with Foreign Ownership, Control, or Influence, or FOCI”.

FAR Subpart 4.4 also specifies responsibilities of Contracting Officers in the pre-solicitation, solicitation, and award phases. Importantly, FAR Subpart 4.4 requires the insertion of the Security Requirements clause, 52.204-2 in solicitations and contracts when access to classified information is required.

Security Requirements Clause

The Security Requirements clause 52.204-2, prescribed in FAR Subpart 4.404, must be inserted in the contracts classified as Confidential, Secret, or Top Secret.

The contract must state that the contractor shall comply with the Security Agreement, DD Form 441, including the NISPOM (DoD 5220.22-M) and any revisions to that manual. It also states that if there are changes by the Government to the security classification or security requirements under the contract that cause a change in security costs of other terms of the contract, then the contract shall be subject to an equitable adjustment.

Finally, the Security Requirements clause must state that the contractor agrees to insert terms and language of this clause in all subcontracts under this contract that involve access to classified information. It is important to note that any additional security requirements outside the scope of the NISPOM must be addressed in each contract that has such requirements. For example, the official contract will detail those security requirements such as types of required clearances, methods of storing information, and so on. Industry must follow every security guideline provided in their contract.

Classification Management

Now that you understand the contractual security requirements, let's examine what classification management means. There are three keys to classification management. The first is having a system of classifying. What needs to be protected? Next, you must define safeguarding. How much protection is required? This answer derives from the definitions associated with Top Secret, Secret, and Confidential. The third key to classification management is declassification of national security information. How long should we protect that information?

One of the responsibilities the Government agrees to is to provide appropriate classification guidance. How else will the contractor know what to protect or how to protect something if they don't know it is classified? The contractor, once they know what is classified and at what level, agrees to establish appropriate security procedures for the protection of that information.

Classification management in the NISP is a joint responsibility. You cannot assume that because a company once was cleared at a certain level, working on a specific contract with appropriate security protections, that the company is cleared for a

different contract. The key takeaway is, “Trust but verify” the clearance, need-to-know, and storage.

GCA Responsibilities

It is the GCA’s responsibility to trust but verify clearance information and provide classification guidance. The GCA ensures the incorporation of appropriate security requirements in a classified contract, including DD Form 254 and the FAR Security Requirements clause, 52.204-2. The GCA provides continued security classification guidance to the contractor during performance of the contract.

Contractor’s Responsibilities

The contractor’s security requirements responsibilities include establishing the appropriate security procedures for the protection of classified information in accordance with the NISPOM guidelines and the Security Agreement, DD Form 441.

The Facility Security Officer (FSO) adheres to NISPOM Guidelines by implementing facility procedures to govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information. FSOs also ensure procedures for implementing and maintaining security-related software for the detection of malicious code, viruses, and intruders, and reporting security incidents.

The contractor notifies the originator of the classification guides when information suggests the need for change in instructions and challenges inconsistent with classification guidance, if necessary. If a contractor awards a subcontract that authorizes the subcontractor to use the Defense Technical Information Center (DTIC), the DD Form 254 provided by the prime to the subcontractor must stipulate the highest category of classification allowable for extraction of information and research accessible from DTIC. Additionally, the prime contractor must submit to DTIC, through the sponsoring GCA, the Registration for Scientific and Technical Information Services, DD Form 1540, prepared under the subcontract.

Security Requirements for Contractors

Contractors in Different Environments

Security requirements for contractors vary depending on the environment in which the classified work will take place. Regardless of where the classified work takes place, at a minimum, the facility must adhere to the NISP and the prescribed requirements, restrictions, and other safeguards defined in the NISPOM to prevent unauthorized disclosure of classified information. However, there may be additional requirements if the work takes place at a government installation or facility.

When a contractor performs work at a government facility, the contract may require it to adhere to the security procedures associated with that particular installation or agency. When work on a classified contract is performed at the contractor's cleared facility, guidance in the NISPOM applies.

Facility Clearance (FCL)

A facility in which classified work will take place must be sponsored for a facility clearance (FCL) if the facility does not already possess one at the appropriate level. Authorized sponsors include the GCA; a cleared defense contractor; a foreign government ally; or a cleared foreign contractor. Note, however, that a contractor cannot sponsor itself for an FCL.

Responsible classification management begins with justification of the security clearance for a company and its employees. The sponsor for the FCL must include a justification, with information regarding the nature of the tasks or services to be performed by the company that require access to classified information.

The most common and preferred justification for an FCL is the DD 254, Contract Security Classification Specification. Other justifications for the FCL include: a Security Aspects Letter; the contract or Statement of Work; a Request for Proposal or Request for Quotation; or a Cooperative Research & Development Agreement (CRADA).

DSS approves or rejects FCLs. The most common reason for FCL rejection is that GCA authorization is not provided. This authorization can be in the form of an email from the GCA, a GCA signature on the DD Form 254, or a separate letter from the GCA.

FCL Security Requirements

An approved FCL does not necessarily equate to cleared storage capabilities. A Government Agency or another contractor must verify through the Industrial Security Facilities Database (ISFD) the facility's clearance level AND the level of approved storage prior to releasing any classified material to a contractor.

DSS verifies the Personnel Security Clearances (PCLs) in connection with granting or maintaining the FCL and ensures Key Management Personnel, including the senior management official and the FSO, are cleared to the level of the FCL. The government activity or cleared contractor would need to verify the PCL of anyone for whom they provide access to classified information, such as a classified visitor. Note, when NISPOM Change 2 is signed, the Insider Threat Senior Official must also be cleared in connection with the FCL.

Contractors may designate employees who require access to classified information during the negotiation of a contract or the preparation of a bid or quotation pertaining

to a prime contract or a subcontract to be processed for PCLs concurrent with the FCL.

The Industrial Security Representative (IS Rep) determines the necessity for a multiple facility organization's branch offices and divisions to be cleared. In these cases, the home office executes the Security Agreement with the Government.

Contractor Security Requirements: Dos and Don'ts

There are some security requirements that can be asked of the contractor and others that cannot. Contractors can only be required to meet security requirements in the NISPOM unless the GCA has included requirements in the contract that are in addition to the baseline requirements of the NISPOM. The Government cannot ask for security requirements that have not been stipulated in the contract and described in DD Form 254 or other contractual documents.

Recall that a procuring activity of the Government, or cleared contractor in the case of subcontracting, may request the FCL in furtherance of a legitimate U.S. Government requirement. Once sponsored, the DSS, GCA and contractor work together to meet following security clearance request requirements.

The contractor must provide a CAGE Code and sign DD Form 441, Department of Defense Security Agreement. The contractor must also complete a Certificate Pertaining to Foreign Interests and identify Key Management Personnel clearances. The contractor is required to implement and enforce the security controls necessary to prevent unauthorized disclosure of classified information, and to provide classified information only to those possessing need-to-know and a valid security clearance. Finally, the contractor must submit to periodic security vulnerability assessments.

Privity of Contract

Some contracts entail a different prime contractor as well as subcontractors. Privity of contract refers to the direct relationship that exists between contracting parties.

The Government has a contract with the prime contractor. Therefore, there is privity of contract between the Government and the prime contractor. The prime contractor has a contract with its subcontractors, so privity of contract exists between the prime contractor and its subcontractors.

The Government, however, does not have a contract with the subcontractor, so privity of contract does not exist between the two parties. Since no privity of contract exists, the Government cannot negotiate directly with the subcontractor or direct the subcontractor to take any action.

Conversely, when privity of contract does exist, parties to the contract can negotiate and require action. The prime contractor is responsible for creating the classified subcontract

with DD Form 254 and ensuring the subcontractor abides by the security requirements defined in the NISPOM as it provides the necessary service or product for the prime's classified contract. Certain security accesses may be in the prime to subcontractor contracts, such as COMSEC, RD, SCI, SAP, NATO, and FGI. It is important to note, though, that the GCA must first approve that access by the subcontract. Failure to meet the contractual security requirements enables the Government to seek remedy against the prime contractor due to privity of contract. While the Government has an interest in the activities and performance of the subcontractors, you must be careful not to violate the contractual relationship.

Review Activities

Review Activity 1

Indicate the policy to which the description applies.

For each statement, select the best response. Check your answers in the Answer Key at the end of this Student Guide.

Question 1 of 3.

Prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information

- FAR Subpart 4.4
- FAR Clause 52.204-2
- NISPOM

Question 2 of 3.

Specifies DoD publications that implement the NISP and provides uniform policies and procedures for acquisition, including contractual security requirements.

- FAR Subpart 4.4
- FAR Clause 52.204-2
- NISPOM

Question 3 of 3.

States that contracts classified as Confidential, Secret, or Top Secret must incorporate the Security Requirements statements.

- FAR Subpart 4.4
- FAR Clause 52.204-2
- NISPOM

Review Activity 2

Indicate whether the responsibility belongs to the GCA or contractor.

For each statement, select the best response. Check your answers in the Answer Key at the end of this Student Guide.

Question 1 of 4.

Ensures DD Form 254 and the FAR Security Requirements clause is incorporated in the contract.

- Government Contracting Activity (GCA)
- Contractor

Question 2 of 4.

Provides on-going security classification guidance throughout the contract performance period

- Government Contracting Activity (GCA)
- Contractor

Question 3 of 4.

Establishes and implements facility procedures in accordance with the NISPOM and DD Form 441

- Government Contracting Activity (GCA)
- Contractor

Question 4 of 4.

Submits the Registration for Scientific and Technical Information Services, DD Form 1540, if DTIC use is required for contract performance

- Government Contracting Activity (GCA)
- Contractor

Review Activity 3

Which of the following are security requirements for contractor participation in classified contracts?

Select all that apply. Check your answers in the Answer Key at the end of this Student Guide.

- Adherence to the NISPOM Guidelines
- Facility clearance at the level stipulated in the contract
- Personnel security clearance for all employees
- Comply with security requirements in the Contract Security Classification Specification

Review Activity 4

Which of the following are security requirements the Government cannot require of the prime contractor?

Select all that apply. Check your answers in the Answer Key at the end of this Student Guide.

- Personnel security clearances for all employees working on the classified contract
- Implement a security control on the information system that was not identified in the contractual documents but is essential to mitigate a new cyber threat
- To sponsor its own Facility Clearance at the level stipulated in the contract
- To schedule a meeting at the subcontractor's cleared facility between the Government and the subcontractor to discuss performance and security issues on the subcontract

Conclusion

Lesson Summary

You have completed the Security Requirements and Guidance lesson.

Answer Key

Review Activity 1

Prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information

- FAR Subpart 4.4
- FAR Clause 52.204-2
- NISPOM (correct response)

Feedback: The NISPOM, in accordance with Executive Order 12829, National Industrial Security Program, and stipulated in FAR Subpart 4.4, prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information.

Specifies DoD publications that implement the NISP and provides uniform policies and procedures for acquisition, including contractual security requirements.

- FAR Subpart 4.4 (correct response)
- FAR Clause 52.204-2
- NISPOM

Feedback: FAR Subpart 4.4 specifies DoD publications that implement the NISP, including the NISPOM, the Industrial Security Regulation, and DoD guidance on foreign ownership. The overarching purpose of the FAR is to provide uniform policies and procedures for acquisition.

States that contracts classified as Confidential, Secret, or Top Secret must incorporate the Security Requirements statements.

- FAR Subpart 4.4
- FAR Clause 52.204-2 (correct response)
- NISPOM

Feedback: The Security Requirements clause 52.204-2, prescribed in FAR Subpart 4.404, must be inserted in the contracts classified as Confidential, Secret, or Top Secret.

Review Activity 2

Ensures DD Form 254 and the FAR Security Requirements clause is incorporated in the contract.

- Government Contracting Activity (GCA) (correct response)
- Contractor

Feedback: *The GCA ensures DD Form 254 and the FAR Security Requirements clause is incorporated in the contract.*

Provides on-going security classification guidance throughout the contract performance period

- Government Contracting Activity (GCA) (correct response)
- Contractor

Feedback: *The GCA provides on-going security classification guidance throughout the contract performance period.*

Establishes and implements facility procedures in accordance with the NISPOM and DD Form 441

- Government Contracting Activity (GCA)
- Contractor (correct response)

Feedback: *The contractor is responsible for implementing facility procedures to safeguard classified information in accordance with the NISPOM and DD Form 441.*

Submits the Registration for Scientific and Technical Information Services, DD Form 1540, if DTIC use is required for contract performance

- Government Contracting Activity (GCA)
- Contractor (correct response)

Feedback: *It is the contractor's responsibility to submit DD Form 1540 through the GCA for DTIC certification and approval for a subcontractor to use DTIC for the extraction of classified information.*

Review Activity 3

Which of the following are security requirements for contractor participation in classified contracts?

- Adherence to the NISPOM Guidelines (correct response)
- Facility clearance at the level stipulated in the contract (correct response)

- Personnel security clearance for all employees
- Comply with security requirements in the Contract Security Classification Specification (correct response)

Feedback: Contractors participating in classified contracts must adhere to the NISPOM guidelines, have an FCL as stipulated in the contract, and comply with the DD Form 254 security requirements.

Review Activity 4

Which of the following are security requirements the Government cannot require of the prime contractor?

- Personnel security clearances for all employees working on the classified contract
- Implement a security control on the information system that was not identified in the contractual documents but is essential to mitigate a new cyber threat (correct response)
- To sponsor its own Facility Clearance at the level stipulated in the contract (correct response)
- To schedule a meeting at the subcontractor's cleared facility between the Government and the subcontractor to discuss performance and security issues on the subcontract (correct response)

Feedback: The Government cannot require the prime contractor to implement a security control not specified in the contract. It also cannot require the prime to sponsor its own FCL as that is not allowed. Finally, the Government cannot ask the prime to essentially allow it to negotiate directly with the subcontractor; or direct the subcontractor to take any action on performance or security issues.

Student Guide

Acquisitions and Contracting Basics in the National Industrial Security Program (NISIP)

Lesson 4: Contract Administration and Security

Contents

Introduction	3
Objectives.....	3
Contracting Process and Security	3
Contracting Process	3
Pre-Award Phase.....	5
Post-Award Phase	7
Contract Management	8
Contract Closeout.....	8
Security in the Contracting Process	8
Security-Related Contractual Documents.....	9
DD Form 254.....	9
DD Form 254: Who Prepares It and When?.....	10
DD Form 441	10
Standard Form 328.....	11
Statement of Work and Performance Work Statement	11
Relationship between Work Statements and the DD Form 254.....	11
Statement of Work (SOW)	11
Performance Work Statement (PWS)	12
Difference between the SOW and PWS.....	12
Review Activities	12
Review Activity 1	12

Review Activity 2	14
Review Activity 3	14
Review Activity 4	15
Conclusion	16
Lesson Summary.....	16
Activity Key	16
Review Activity 1	16
Review Activity 2	17
Review Activity 3	18
Review Activity 4	19

Introduction

Objectives

In this lesson, you will delve into the contract administration process and security-related contractual documents.

Here are the lesson objectives:

- Identify the phases of contract administration and the impact of security requirements in the contracting process
 - Identify the activities in the contracting process phases
 - Identify the considerations and impact of security requirements during the contracting process phases
- Identify the purpose of the security-related contractual documents: DD Form 254, DD Form 441, SF 328
- Identify the relationship of the SOW or PWS to DD Form 254
 - Identify the purpose of the Statement of Work
 - Identify the purpose of the Performance Work Statement
 - Differentiate the SOW from a PWS

Contracting Process and Security

Contracting Process

Across the DoD acquisition life cycle multiple contracts for the procurement of services or a weapon system product can occur. Each contract follows a four-phased approach known as the contracting process or contract administration. The contracting process begins after the program enters Milestone A. Every acquisition, and its resulting contract, follows these four phases: Pre-Award, Post-Award, Contract Management, and Contract Closeout. The Federal Acquisition Regulation (FAR) is the principal regulatory guidance for implementing procurements and contracts.

Since industrial security involves both the Government and industry working closely together, it is important that both parties understand and document all details, such as security provisions and deliverable dates, prior to beginning the effort. Having written expectations in a contract allows everyone involved to follow the contract appropriately.

During the Pre-Award phase, acquisition planning, issuing the solicitation, and source selection occur. The Contracting Officer and the Contracting Officer's

Representative (COR), if appointed, work closely with the Program Manager, DoD Security Specialists, and the Systems Security Engineering (SSE) group to define the requirements and prepare the Request for Proposal (RFP).

During the Post-Award phase, the Government and the Contractor meet and prepare to implement the contract.

In the Contract Management phase, the Contractor provides the agreed-upon product or service. While the COR closely monitors Contractor performance, the GCA works with the FSO and Information System Security Manager (ISSM) to monitor and mitigate threats and vulnerabilities. The GCA also works closely with members of the SSE group.

During the Contract Closeout phase, the Government provides final acceptance and payment, and submits the Contractor performance evaluation. FAR 4.804, Closeout of Contract Files, details the various closeout tasks that must be completed.

Systems Security Engineering (SSE)

Security for complex weapon systems requires a variety of subject matter experts. Systems Security Engineering is performed by a variety of professionals, from Government and Industry, to ensure a comprehensive analysis of system technology, hardware, software, firmware, and information, including:

- Systems Engineers (SEs)
- SSE Subject Matter Experts (SMEs)
- Logistics
- System user representatives
- Supporting counterintelligence, intelligence, foreign disclosure, and security personnel

SSEs play an important role in Pre-System Acquisition, System Acquisition and Sustainment activities.

Here are important security-related activities performed by the SSEs in the acquisition life cycle phases:

- Pre-System Acquisition:
 - Participate in contract preparation and source selection to ensure security concerns are addressed and included in proposals, source evaluations and contract negotiations and cost discussions

- Perform an initial Criticality Analysis (CA) based on mission threats and system functions
- System Acquisition:
 - Update criticality assessment, risk, threat and mitigation as required
 - Ensure all Critical Program Information (CPI) and mission-critical functions are identified and associated countermeasures applied
- Sustainment
 - Programs with Critical Program Information (CPI) require continued evaluation and monitoring as protection and threat / vulnerability / countermeasures may have to continue to evolve.

Pre-Award Phase

The Pre-Award phase involves all activities associated with identifying and justifying a mission need, formulating an acquisition strategy to meet this need, and implementing the strategy by means of a contractual relationship with the private sector. The objective at the end of the Pre-Award phase is to select the proposal that represents the best value to the Government. The contracting process is a partnership between the contracting office and program personnel. The Contracting Officer molds and shapes the procurement and is ultimately responsible for contract award and administration.

The Pre-Award phase incorporates three stages: pre-solicitation, solicitation, and source selection. The participation of contractual, security, and technical subject matter experts is essential to managing and completing this phase of the contracting process. If access to classified material is a requirement during the pre-award phase, then the contractor must have a Facility Clearance (FCL) and safeguarding capability. If a contractor is not cleared or they do not have the appropriate safeguarding capability, the Government Contracting Activity (GCA) or a cleared prime, must sponsor the contractor for a facility security clearance by submitting a sponsorship letter to DSS, which will then allow the contractor to bid on the contract.

Pre-Solicitation

The Pre-Solicitation stage has two major steps.

- Requirements Definition activities include gathering technical data to meet the needs, performing market research, defining the Statement of Objectives (SOO) and then preparing either the SOW or PWS, and identifying the contracting method.

- The SOO is the portion of a contract that establishes a broad description of the Government's required performance objectives. The SOO informs the preparation of the SOW or PWS. The PWS or SOW become part of the contract.
- Method of Contracting can be sealed bid as defined in FAR 6.401 or contracting by negotiation defined FAR 15
- Acquisition Strategy describes:
 - What the basic contract buys
 - How the items are defined
 - Options, if any, and prerequisites for exercising them
 - Events established in the contract to support appropriate exit criteria for the phase or immediate development activity.
 - Market research
 - Competition
 - Incentive strategies needed to promote the attainment of selected program priorities, such as cost and/or schedule goals.

DFARS 207.105 describes the required contents of written acquisition plans.

Solicitation

The Solicitation stage is concerned with contract formulation. There are three solicitation types: Request for Proposal (RFP), Request for Quote (RFQ), Invitation for Bid (IFB).

Acquisitions over the simplified acquisition threshold, use the Request for Proposal (RFP). It is a formal negotiated solicitation that results in a formal contract award. A successful project depends on a detailed, specific RFP that clearly outlines the deliverable and its requirements. The RFP must clearly define the evaluation criteria by which the contractor's proposal will be judged.

Source Selection

The Source Selection Stage is required for all best-value, negotiated, competitive acquisitions under FAR Part 15. There are two steps in the stage: Evaluation and Contract Award. The vision for the Federal Acquisition System is to deliver, on a timely basis, the best value product or service to the customer. This is accomplished by using contractors who have a track record of successful past performance or who demonstrate a current superior ability to perform a contract.

The Source Selection stage has two major steps: Evaluation and Contract Award.

- Evaluation
 - Is an assessment of the:
 - Contractor's proposal based on criteria stated in the solicitation (e.g., RFP)
 - Offeror's ability to perform the prospective contract successfully
 - Conducting the evaluation is tailored based on whether the tradeoff, lowest price and technically acceptable (LPTA), or sole-source approach is used.
 - Tradeoff - Source Selection Process allows for a tradeoff between non-cost factors and cost/price and allows the Government to accept other than the lowest priced proposal or other than the highest technically rated proposal to achieve a best-value contract award.
 - Lowest Price and Technically Acceptable - Source Selection Process appropriate when best value is expected to result from selection of a technically acceptable proposal with the lowest evaluated price.
- Contract Award
 - Requires completion of final evaluations and approval of the required clearance documentation
 - GCA notifies the contractor of the award and it is published in FedBizOpps
 - Written notification to each unsuccessful offeror is sent

Post-Award Phase

Key activities in the Post-Award phase include setting up the contract file as required in FAR 4.803, preparing the Management Plan based on the contract by specifying contractor tasks and deliverables outlined in the SOW or PWS and describing how the Government will conduct inspection and acceptance of the contractor's performance, and conducting the post-award orientation meeting to present all contract requirements to the Contractor and gain mutual understanding. This

meeting brings the stakeholders together to clarify the performance expectation, inspection and acceptance criteria, invoicing and payments, and schedules.

For contracts requiring access to classified information with defined security requirements in the contract's DD Form 254, DoD Security Specialists may be invited to the meeting to address those requirements and any concerns.

Contract Management

Activities during the Contract Management phase revolve around meeting the performance, cost, and schedule requirements in the contract. Government and contractor security professionals must also continuously manage the risks.

DSS oversees contractor compliance with the NISPOM when the classified work is performed at a cleared contractor facility. The FSO is responsible for enforcing any and all security requirements at the contractor's site as specified in the contract, which includes adhering to the NISPOM. Contractors can expect periodic reviews from the IS Rep to ensure compliance with all security requirements specified in the classified contract.

When contractors work at government installations, security considerations include establishing or maintaining personnel security clearances, safeguarding classified material, facility access control, and/or preparing for classified visits. There may be additional security requirements and protocols to which contractor employees must adhere. Communication between the security professionals and DSS is important to minimizing risk and remaining aware of new vulnerabilities and threats to DoD systems. Security Specialists assist in revisions to the DD Form 254 when there are changes to any classification guidance.

Contract Closeout

To closeout a contract, the Contracting Officer must ensure that the work conforms to the requirements in the SOW or PWS. Any deficiencies must be resolved before final payment is made. Within two years of contract completion, the contractor must either return or dispose of classified material received or generated under the contract to the GCA. The GCA may authorize holding the material longer if there is a legitimate reason. Finally, a final DD Form 254 must be completed.

Once the product or service is accepted, badges are collected and system access and security clearances are cancelled.

Security in the Contracting Process

Recall that during the Pre-Solicitation stage of the Pre-Award phase, the GCA raises the security issues that the contract should address. The local security office should be involved in developing the security requirements. The Government Program

Manager should be included in this process. The PM understands the program requirements and can help to articulate contract and security requirements. Remember, the level of security required on a contract will affect the cost of the contract, so key questions to ask and answer include the following. What FAR security contract clauses should be incorporated? What are the legitimate security needs related to a program?

Since multiple contracts may be required as a program moves through the acquisition life cycle, the GCA must consider which contracts need to be classified and at what level.

By the time a solicitation is released, there should be a clear understanding of the security requirements and they should be incorporated in the RFP's SOW or PWS and in the DD Form 254. As security requirements change, these changes should be communicated to the contractors and contracts may be modified based on increased or decreased costs. Communication between the Contracting Officer and the FSO is very important for managing the inherent risks of changing security requirements..

FAR 52.204-2

Classified contracts must include FAR 52.204.2 and the DD Form 254. All "Classified Contracts" must have, at a minimum, the Clause 52.204-2, Security Requirements, incorporated into the contract. The FAR also requires use of a DD Form 254, Contract Security Classification Specifications, for classified contracts.

If the contractor then subcontracts the work, they are obligated, under the National Industrial Security Program, to pass those requirements on to the subcontract.

Contracts requiring work that is unclassified but sensitive should also be evaluated to ensure that contractors have undergone an appropriate level of background investigation to perform the required duties, and contractors must be made aware of any procedures or requirements regarding proper protection of unclassified but sensitive information.

Security-Related Contractual Documents

DD Form 254

The Contract Security Classification Specification, DD Form 254, is part of the solicitation package. It is a contractually binding document to provide the contractor with the security requirements and classification guidance needed for performance on a classified contract. It also identifies the requirement to generate and store classified information at a contractor facility and, as one of three sources, it may be used for derivative classification. DD Form 254 advises the contractor on handling procedures for classified material received or generated. Finally, it provides guidance

on any special security requirements above and beyond those required by the NISPOM and how to handle public disclosure.

Block 1 addresses the FCL and safeguarding requirement and provides the contractor with specific clearance and access requirements for contracts requiring access to or creating classified information. Block 10 defines what access the contract requires. Block 11 specifies what the contractor will need to do in performing the contract.

DD Form 254: Who Prepares It and When?

The initial DD Form 254, embedded in the solicitation package, is prepared by the GCA, subject matter experts, and the Security Specialist. There are 17 blocks of information on the form.

As a recommended best practice, preparing DD Form 254 is most often a team effort including the following: Security Office and OPSEC Program Office; Contracting Office; and Project Office and Technical Team.

This binding document is between the Government and the Prime Contractor. The prime contractor contracts with sub-contractors.

There are a minimum of three versions of DD Form 254: the Original submitted with the RFP; the Original submitted with the Contract Award; and the Final DD Form 254 submitted at Closeout. A revised DD Form 254 is issued whenever there are changes to any classification guidance previously provided.

Block 13 defines the security guidance and clarifies previous reference items. Block 14 specifies any additional requirements, while Block 15 indicates what entity has inspection responsibility.

More information on common security-related contract clauses and their associated FAR security clauses, as well as a guide for preparing the DD Form 254 can be accessed in the Course Resources.

DD Form 441

The DD Form 441, Department of Defense Security Agreement, is an agreement between the contractor's organization and the United States Government. By signing the security agreement, the contractor makes a commitment to establish and maintain a security program that is in compliance with the requirements found in the NISPOM.

The six sections of the agreement detail the security responsibilities of both the cleared organization and the United States Government. The contractor submits DD Form 441 as part of the process to obtain an FCL. If the contractor is a multiple-

facility organization with divisions at different FCL levels, then the home office executes the Security Agreement. DD Form 441-1 is an attachment to the DD Form 441 that lists cleared divisions or branch offices that are included in and covered by the provisions of the organization's Security Agreement and Certificate Pertaining to Foreign Interest. In the parent company/subsidiary facility structure, DD Form 441 is required.

Standard Form 328

The Standard Form, or SF, 328, Certificate Pertaining to Foreign Interests, is required whenever a cleared company enters into discussions, consultations, or agreements that may reasonably lead to effective ownership or control of the company by a foreign interest. It must be submitted to DSS in writing during the initial facility clearance process and when significant changes occur to information previously forwarded.

The purpose of the SF 328 is to prevent: unauthorized access to classified information and to prevent any company operations and management that may adversely affect the performance of classified contracts.

In a corporate family, the SF 328 should be a consolidated response rather than separate submissions from individual members of the corporate family. In the case of an organization with multiple tiers of parent-subsiary relationships, the SF 328 should be certified by the highest tier cleared entity.

Statement of Work and Performance Work Statement

Relationship between Work Statements and the DD Form 254

Recall that a solicitation package released for bid to industry contains either an SOW or a PWS, as well as the DD Form 254, that defines the security requirements. In this example, the GCA chose the PWS that defines performance outcomes for the service or product.

When the work to be performed is on a classified contract, the solicitation package must include both documents so that the contractor has a clear understanding of not only the product or service, but also the security requirements.

Statement of Work (SOW)

The purpose of the SOW is to describe not only what is to be done, but also how it is to be done. By describing the work in such detail, the government essentially provides the preferred approach or solution to the problem. This effectively locks in the approach the contractor must take.

The SOW contents include background on the requirement and the objective of the work or the desired end product. It provides the scope of the work required by the acquisition of a nontechnical nature with step-by-step task requirements and the resulting final product for each task or phase.

The SOW defines who will work on the project and the clearance levels required. Finally, the SOW will state required travel, if applicable.

Performance Work Statement (PWS)

The purpose of the PWS is three-fold. First, it states the work to be performed in terms of outcomes or results. It does not prescribe the contractor's method of performance. Second, the PWS defines measurable standards and financial incentives in a competitive environment to encourage innovation and cost-effective methods of performing the work. Finally, the purpose of the PWS is to provide a method to assess contractor performance. This requires a Quality Assurance Surveillance Plan (QASP).

Typically, the PWS contents include a brief description of the service or product, background, and the objectives. It will provide the scope of the work, period of performance and quality control measures. Finally, it provides the required QASP, by which the standards established in the scope of the work are measured.

Difference between the SOW and PWS

Placed on a continuum, the PWS is less detailed and prescriptive than the SOW. Much of the risk is shifted to the contractor. The PWS is the preferred approach by the Government because it encourages innovation and cost-effective methods of performing the work. However, the SOW is useful when the task is well-known and can be described in specific terms.

Examining the difference between the PWS and SOW approaches, the risk burden shifts to the contractor when the Government uses the PWS. The SOW is not without risk. There is risk for the Government when using the SOW approach. The danger is that if the contractor follows the Government's step-by-step SOW and the result is unacceptable, it is the Government's fault.

Review Activities

Review Activity 1

Identify the contracting phase for each of the following statements.

For each statement, select the best response. Check your answers in the Answer Key at the end of this Student Guide.

Question 1 of 4.

During this phase, the GCA works with the FSO and ISSM to monitor and mitigate threats and vulnerabilities.

- Pre-Award Phase
- Post-Award Phase
- Contract Management Phase
- Closeout Phase

Question 2 of 4.

During this phase, the program stakeholders come together to review the contract performance requirements and security issues.

- Pre-Award Phase
- Post-Award Phase
- Contract Management Phase
- Closeout Phase

Question 3 of 4.

During this phase, the solicitation is released with the FAR Security Requirements Clause for classified contracts.

- Pre-Award Phase
- Post-Award Phase
- Contract Management Phase
- Closeout Phase

Question 4 of 4.

During this phase, all classified material must be returned to the GCA or destroyed.

- Pre-Award Phase
- Post-Award Phase
- Contract Management Phase
- Closeout Phase

Review Activity 2

For each statement, select True or False. Check your answers in the Answer Key at the end of this Student Guide.

Question 1 of 3.

The DD Form 254 is required for classified contracts and submitted to the contractor at the Post-Award orientation meeting.

- True
- False

Question 2 of 3.

DSS involvement in the contracting process occurs once the classified contract is awarded.

- True
- False

Question 3 of 3.

The level of security required on a contract will affect the cost of the contract, so as security requirements change, contracts may be modified based on increased or decreased costs.

- True
- False

Review Activity 3

Identify the contractual document for each purpose statement.

For each statement, select the best response. Check your answers in the Answer Key at the end of this Student Guide.

Question 1 of 3.

Defines what the contractor agrees to do and what the Government agrees to do regarding security responsibilities as part of the FCL process

- DD Form 254
- DD Form 441
- SF 328

Question 2 of 3.

Provides a contractor with the security requirements and classification guidance needed for performance on a classified contract

- DD Form 254
- DD Form 441
- SF 328

Question 3 of 3.

Prevents unauthorized access to classified information and prevents any company operations and management that may adversely affect the performance of classified contracts

- DD Form 254
- DD Form 441
- SF 328

Review Activity 4

Identify the work statement approach for each description.

For each statement, select the best response. Check your answers in the Answer Key at the end of this Student Guide.

Question 1 of 3.

The contractor will use the Workflow Management System to monitor, update, and report on the status of assigned tasks every 12 hours with 98% data accuracy in tracking.

- Performance Work Statement
- Statement of Work

Question 2 of 3.

The contractor will provide cyber analysis and develop documentation necessary to develop future campaign plans, operational, and contingency plans.

- Performance Work Statement
- Statement of Work

Question 3 of 3.

This work statement approach shifts the risk to the contractor while encouraging innovative and cost-effective methods to accomplish the work.

- Performance Work Statement
- Statement of Work

Review Activity 5

In which of the following contractual documents would this statement likely be included?

“This contract may involve handling and storage of classified material. Contractor has responsibility for alarmed areas and properly escorting both contractor and government visitors.”

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- DD Form 441, DoD Security Agreement
- DD Form 254 Contract Security Classification Specification
- Performance Work Statement (PWS)
- Statement of Work (SOW)

Conclusion

Lesson Summary

You have completed the Contract Administration and Security lesson.

Activity Key

Review Activity 1

Question 1 of 4.

During this phase, the GCA works with the FSO and ISSM to monitor and mitigate threats and vulnerabilities.

- Pre-Award Phase
- Post-Award Phase
- Contract Management Phase (correct response)
- Closeout Phase

Feedback: *During the Contract Management phase, the GCA works with the FSO and ISSM to monitor and mitigate threats and vulnerabilities.*

Question 2 of 4.

During this phase, the program stakeholders come together to review the contract performance requirements and security issues.

- Pre-Award Phase
- Post-Award Phase (correct response)
- Contract Management Phase
- Closeout Phase

Feedback: During the Post-Award phase, the program stakeholders come together to review the contract performance requirements and security issues.

Question 3 of 4.

During this phase, the solicitation is released with the FAR Security Requirements Clause for classified contracts.

- Pre-Award Phase (correct response)
- Post-Award Phase
- Contract Management Phase
- Closeout Phase

Feedback: During the Pre-Award phase, the solicitation is released with the FAR Security Requirements Clause for classified contracts.

Question 4 of 4.

During this phase, all classified material must be returned to the GCA or destroyed.

- Pre-Award Phase
- Post-Award Phase
- Contract Management Phase
- Closeout Phase (correct response)

Feedback: During the Closeout phase, all classified material must be returned to the GCA or destroyed.

Review Activity 2

Question 1 of 3.

The DD Form 254 is required for classified contracts and submitted to the contractor at the Post-Award orientation meeting.

- True
- False (correct response)

Feedback: DD Form 254 is required for classified contracts and is part of the solicitation package released during the Pre-Award phase.

Question 2 of 3.

DSS involvement in the contracting process occurs once the classified contract is awarded.

- True
- False (correct response)

Feedback: DSS is involved throughout the contracting process by providing input on security requirements and if a contractor is not cleared or they do not have the appropriate safeguarding capability, the GCA or a cleared prime, must sponsor the contractor for a facility security clearance by submitting a sponsorship letter to DSS, which will then allow the contractor to bid on the contract.

Question 3 of 3.

The level of security required on a contract will affect the cost of the contract, so as security requirements change, contracts may be modified based on increased or decreased costs.

- True (correct response)
- False

Feedback: The level of security required on a contract will affect the cost of the contract, so as security requirements change, contracts may be modified based on increased or decreased costs.

Review Activity 3

Question 1 of 3.

Defines what the contractor agrees to do and what the Government agrees to do regarding security responsibilities as part of the FCL process

- DD Form 254
- DD Form 441 (correct response)
- SF 328

Feedback: DD Form 441 defines what the contractor agrees to do and what the Government agrees to do regarding security responsibilities as part of the FCL process.

Question 2 of 3.

Provides a contractor with the security requirements and classification guidance needed for performance on a classified contract

- DD Form 254 (correct response)

- DD Form 441
- SF 328

Feedback: DD Form 254 provides a contractor with the security requirements and classification guidance needed for performance on a classified contract and is part of the solicitation package.

Question 3 of 3.

Prevents unauthorized access to classified information and prevents any company operations and management that may adversely affect the performance of classified contracts

- DD Form 254
- DD Form 441
- SF 328 (correct response)

Feedback: The purpose of the SF 328 is to prevent unauthorized access to classified information and any company operations and management that may adversely affect the performance of classified contracts.

Review Activity 4

Question 1 of 3.

The contractor will use the Workflow Management System to monitor, update, and report on the status of assigned tasks every 12 hours with 98% data accuracy in tracking.

- Performance Work Statement
- Statement of Work (correct response)

Feedback: This is an SOW statement that specifically defines how the contractor will do the task.

Question 2 of 3.

The contractor will provide cyber analysis and develop documentation necessary to develop future campaign plans, operational, and contingency plans.

- Performance Work Statement (correct response)
- Statement of Work

Feedback: This is a PWS statement that expresses the required outcomes. It does not tell the contractor how to do the analysis or prescribe what the documentation format should be.

Question 3 of 3.

This work statement approach shifts the risk to the contractor while encouraging innovative and cost-effective methods to accomplish the work.

- Performance Work Statement (correct response)
- Statement of Work

Feedback: *The PWS is less detailed and prescriptive which enables the contractor to use innovative and cost-effective methods to accomplish the work. The burden of risk is on the contractor to deliver a service or product acceptable to the Government on time.*

Review Activity 5

In which of the following contractual documents would this statement likely be included?

“This contract may involve handling and storage of classified material. Contractor has responsibility for alarmed areas and properly escorting both contractor and government visitors.”

- DD Form 441, DoD Security Agreement
- DD Form 254 Contract Security Classification Specification (correct response)
- Performance Work Statement (PWS)
- Statement of Work (SOW)

Feedback: *The PWS is less detailed and prescriptive which enables the contractor to use innovative and cost-effective methods to accomplish the work. The burden of risk is on the contractor to deliver a service or product acceptable to the Government on time.*

Student Guide

Acquisitions and Contracting Basics in the National Industrial Security Program (NISP)

Lesson 5: Course Conclusion

Contents

Course Conclusion.....	2
Course Summary.....	2
Lesson Review	2
Course Objectives	2

Course Conclusion

Course Summary

In this course, you learned about the DoD acquisition life cycle, the important role of the NISP for contracts requiring access to classified information, and the process for moving an acquisition through the life cycle. You also examined the security requirements for classified contracts specified by the Federal Acquisition Regulation (FAR) and in the NISPOM as well as the security requirements for contractor participation. Finally, you delved deeper into the phases of the contracting process and the security-related contractual documents, as well as the Statement of Work (SOW) and the Performance Work Statement (PWS) that are part of the solicitation package and awarded contract.

Lesson Review

Here is a list of lessons in the course:

- Lesson 1: Course Introduction
- Lesson 2: DoD Acquisition Life Cycle and Security Requirements
- Lesson 3: Security Requirements and Guidance
- Lesson 4: Contract Administration and Security
- Lesson 5: Course Conclusion

Course Objectives

Congratulations. You have completed the Acquisitions and Contracting Basics course. You should now be able to:

- Identify the phases in the acquisition life cycle
- Identify the role of security professionals in the DoD acquisition life cycle
- Identify the importance of planning for security across the acquisition life cycle and during the contracting process
- Identify the phases of contract administration and the impact of security requirements in the contracting process
- Identify the purpose of the security-related contractual documents: DD Form 254, DD Form 441, SF 328
- Identify the relationship between the Statement of Work and Performance Work Statement to DD Form 254

To receive course credit, you **MUST** take the Acquisitions and Contracting Basics examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to register for the online exam. Otherwise, select the Take Exam button on the last screen of the course to take the online exam and receive your certificate.