Acquisitions and Contracting Basics in the National Industrial Security Program (NISP), Version 4
Student Guide

May 2024

Center for Development of Security Excellence

Lesson 1: Course Introduction

Introduction

Opening

Weapon System PM: 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 (CI): 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 process? 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, Adaptive Acquisition Framework 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:

1. Identify the pathways in the acquisition framework
2. Describe the role of security professionals in the DOD acquisition framework
3. Recognize the importance of planning for security across the acquisition process and during the contracting process

4. Describe the phases of contract administration and the impact of security requirements in the contracting process
5. Describe the purpose of security-related contractual documents
6. Explain the relationship of the Statement of Work (SOW) and Performance Work Statement (PWS) to DD Form 254

Lesson 2: DOD Acquisition Framework and Security Requirements

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 pathways in the acquisition framework
  - Explain the important role of the National Industrial Security Program (NISP) in the acquisition system
  - Describe the process for moving an acquisition through the Adaptive Acquisition Framework (AAF)
- Explain the role of security professionals in the DOD acquisition system
  - Name the key government roles and responsibilities in the DOD acquisition system
  - Describe the key contractor roles and responsibilities in the DOD acquisition system

National Industrial Security Program and the DOD Acquisition Framework

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 32 Code of Federal Regulations Part 117, 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 Framework

The Department of Defense Instruction (DODI) 5000.02 provides guidance on the Operation of the Defense Acquisition System Adaptive Acquisition Framework. The emphasis in this instruction is on tailoring procedures and processes for the individual program's needs.

There are six pathways describing multiple acquisition approaches that provide capability to the user while capitalizing on advanced acquisition methods and improving the DOD's ability to benefit from commercial innovation. The AAF acquisition pathways provide opportunities for Milestone Decision Authority (MDAs/DAs) and Program Managers (PMs) to develop acquisition strategies and employ acquisition processes that match the characteristics of the capability being acquired.

The first pathway is Urgent Capability Acquisition. Its purpose is to field capabilities to fulfill urgent existing or emerging operational needs or quick reactions in less than 2 years. Department of Defense Directive (DODD) 5000.71 and DODI 5000.81 establish policies and provide procedures for urgent operational needs and other quick reaction capabilities acquisition.

The second pathway is Mitigate Tier of Acquisition (MTA). Its purpose is to rapidly develop fieldable prototypes within an acquisition program to demonstrate new capabilities or rapidly field production quantities of systems with proven technologies that require minimal development. DODI 5000.80 establishes policy, assigns responsibilities, and prescribes procedures for the MTA pathway.

The third tier is Major Capability Acquisition. Its purpose is to acquire and modernize military unique programs that provide enduring capability. DODI 5000.85 establishes policy, assigns responsibilities, and prescribes procedures for the Major Capability Acquisition pathway. All major capability acquisition pathway programs are designated by an acquisition category (ACAT). The ACAT identifies the program's MDA, required processes, and documents.

The fourth pathway is Software Acquisition. Its purpose is to facilitate rapid and iterative delivery of software capability to the user. For example, software-intensive systems and software-intensive components or subsystems would fall under this pathway. DODI 5000.87 establishes policy, assigns responsibility, and prescribes procedures for the Software Acquisition pathway.

The fifth pathway is Defense Business Systems (DBS) Acquisition. Its purpose is to acquire information systems that support DOD business operations. DODI 5000.75 establishes policies and provides procedures for the DBS acquisition pathway. This pathway applies to defense business capabilities and their supporting business systems, including those with "as-a-service" solutions. This includes financial and financial data feeder, contracting, logistics, planning and budgeting, installations management, human resources management, and training and readiness systems. It may also be used to acquire non-developmental, software intensive programs that are not business systems.

The sixth pathway is Acquisition of Services. Its purpose is to acquire services from the private sector. This includes knowledge-based, construction, electronics and communications, equipment, facilities, product support, logistics, medical, research and development, and transportation services. DODI

5000.74 and the online Service Acquisition Mall establish policies and provide procedures for the Acquisition of Services pathway.

This lesson will focus on Major Capability Acquisitions and the typical structured approach followed in application of this acquisition pathway.

Milestones and Decision Points

There are five phases in the Major Acquisition Pathway:

- Materiel Solution Analysis
- Technology Maturation and Risk Reduction
- Engineering and Manufacturing Development
- Production and Deployment
- Operations and Support

There are milestone decision reviews embedded within each phase of the pathway to assess a program's readiness to proceed to the next 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. Milestone decision reviews ensure that a sound investment decision committing the Department's financial resources is made.

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 Engineering of Defense Systems Guidebook, Chapter 3, Technical Reviews and Audits.

The first decision point, the Materiel Development Decision (MDD) is the mandatory entry point into the Major Capability Acquisition process and is informed by a validated requirements document - for example, an initial capabilities document (ICD) or equivalent and the completion of the analysis of alternatives (AoA) study guidance and the AoA study plan.

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 phase 2, Technology Maturation and Risk Reduction (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 next decision point, 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.

Next, we will briefly discuss each phase of the Major Capability Acquisition Pathway.

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.

Key activities during Phase 1:

- The identification and analysis of alternatives (AoA), measures of effectiveness, key trades between cost and capability, life-cycle cost, schedule, concepts of operations, and overall risk.
- The AoA will inform and be informed by affordability analysis, sustainment considerations, early systems engineering analysis, threat projections, and coalition interoperability as identified in the ICD.
- An independent cost estimate (ICE) and independent technical risk assessment (ITRA) will be conducted.
- Product support (PS) and sustainment planning begins in support of the determination of core logistics capability requirements.
- Component Acquisition Executive (CAE) selects a Program Manager and establishes a program office to plan the acquisition program with emphasis on the next decision point.

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.

Key activities during TMRR:

- Close collaboration with the requirements community to inform development and validation of the CDD
- Design trades and requirements trades necessary to ensure an affordable product and executable development and production programs are made
- The acquisition strategy will be refined to describe the overall approach to acquiring the capability and include the program schedule, risks, funding, business strategy, and an IP strategy
- PS and sustainment planning continues and will include consideration of data rights
- Program security and program protection requirements will be evaluated

Phase 3: Engineering and Manufacturing Development (EMD)

The purpose of the EMD activities is to develop, build, test, and evaluate a materiel solution to verify that all operational and implied requirements, including those for security, have been met and to support production, deployment and sustainment decisions.

Key activities during EMD:

- Demonstration that the system design (hardware & software) is ready to begin pre-production prototype hardware fabrication or software coding with acceptable risk
- Independent evaluations, operational assessments or limited use test to provide initial assessments of operational effectiveness, suitability, survivability and demonstrate ability to achieve key performance parameters (KPPs) and key system attributes (KSAs)
- Training devices will be planned, funded, designed, and developed in parallel with the operational system to ensure that the training devices properly replicate the capability in development
- Manufacturing processes are effectively demonstrated and are under control

Phase 4: Production and Deployment (P&D)

The purpose of the P&D phase is to produce and deploy requirements-compliant materiel solutions to the receiving operating organizations.

Key activities in P&D:

- LRIP, personnel training, completion of developmental test and evaluation (if required), initial operational test and evaluation, and the full-rate production (FRP) or full-deployment (FD) decision
- All system sustainment and support activities are initiated if not already begun, and the appropriate operational authority will declare initial operational capability (IOC) when the defined operational organization has been equipped and trained and is determined to be capable of conducting mission operations
- "Should cost" management and other techniques will be used continuously to control and reduce costs

Phase 5: Operations and Support (O&S)

This phase executes the PSS, satisfies materiel readiness and operational support performance requirements including personnel training, and sustains the system over its life cycle, including disposal. The O&S phase begins upon fielding of the first system(s), which may precede IOC, and is based on an MDA-approved PSS.

Key activities in O&S:

- 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 PSS
- 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 PSS.
    - Measures, assesses, and reports system readiness using sustainment metrics, and implements corrective actions for trends diverging from the required performance outcomes defined in the APB and the PSS.

- Manage revisions to the PSS as warranted by operational needs, training requirements, technology advances, evolving threats, process improvements, fiscal constraints, plans for follow-on systems, changes to the industrial base, or a combination of these influences.

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.
- Disposal planning will include consideration of retirement, disposition, and reclamation.

Acquisition Management and the NISP

Government security offices are integrated throughout the program and acquisition lifecycle 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 process. 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.

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: Department of Defense, Office of the Director of National Intelligence, Department of Energy, United States Nuclear Regulatory Commission, and Department of Homeland Security. 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 and any applicable Defense Federal Acquisition Regulation Supplements (DFARS). 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 purpose of the DFAR is to provide DOD agency level acquisition regulation supplements.

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 an entity eligibility determination, also referred to as a facility clearance (FCL) and influences potential Foreign Ownership, Control, or Influence, or 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, DCSA, 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 lifecycle 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 (PWS) or Statement of Work (SOW).

The COR assures the contractor maintains an FCL and a favorable national security eligibility determination, also referred to as Personnel Security Clearances (PCL) when access to classified information is required.

CORs communicate the security requirements during the procurement process and contract performance.

Defense Counterintelligence and Security Agency (DCSA)

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

DCSA 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. DCSA conducts security reviews 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.

DCSA 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 NISPOM. The Senior Management Official (SMO) is the contractor's official responsible for the entity policy and strategy. The SMO has ultimate authority over the facility's operations and the authority to direct actions necessary for the safeguarding of classified information in the facility. The Facility Security Officer (FSO) works closely with the DCSA Industrial Security Representative to maintain a viable security program.

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

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

NISP Contract Classification System (NCCS)

The NISP Contracts 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

Activity 1

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.

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

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

Activity 2

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

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

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

Activity 3

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

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

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

Activity 4

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.

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

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

Activity 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.

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

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

Activity 6

The GCA ensures that contracts for classified work include the FAR Security Requirements and DD Form 254.

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

- ○ True
- ○ False

Activity 7

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

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

- ○ True
- ○ False

Activity 8

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

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

- ○ True
- ○ False

Activity 9

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

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

- ○ Contracting Officer's Representative (COR)
- ○ Contracting Officer
- ○ Defense Counterintelligence and Security Agency (DCSA)
- ○ Contractor

Activity 10

Issues subcontracts with the DD Form 254.

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

- ○ Contracting Officer's Representative (COR)
- ○ Contracting Officer
- ○ Defense Counterintelligence and Security Agency (DCSA)
- ○ Contractor

Activity 11

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

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

- ○ Contracting Officer's Representative (COR)
- ○ Contracting Officer
- ○ Defense Counterintelligence and Security Agency (DCSA)
- ○ Contractor

Activity 12

Conducts security reviews on contractors and coordinates with the appropriate DOD representatives and Security Specialists on damage assessments.

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

- ○ Contracting Officer's Representative (COR)
- ○ Contracting Officer
- ○ Defense Counterintelligence and Security Agency (DCSA)
- ○ Contractor

Conclusion

Lesson Summary

You have completed the lesson "DOD Acquisition Framework and Security Requirements."

Lesson 3: Security Requirements and Guidance

Introduction

Objectives

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

Here are the lesson objectives:

- Identify the importance of planning for security across the acquisition process and during the contracting process
- Explain the relationship of contractual security requirements in the FAR and security guidance based on the NISPOM
- Name 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 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 (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 NISPOM.

DOD guidance with respect to foreign ownership is outlined in DOD Manual 5220.32, Volume 2, "National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)" and Directive-type Memorandum (DTM) 15-002, "Policy Guidance for the Processing of National Interest Determinations (NIDs) in Connection with Foreign Ownership, Control, or Influence (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, the NISPOM and any revisions to that NISPOM. 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 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 where the contractor performs work on classified contracts 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.

Entity Eligibility Determination – 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. A contractor or prospective contractor cannot apply for its own FCL. A GCA or a currently cleared contractor may sponsor an entity for FCL at any point during the contracting or agreement life cycle at which the entity must have access to classified information to participate (including the solicitation or competition phase).

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 and Development Agreement (CRADA).

DCSA 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 FCL System of record, the facility's clearance level AND the level of approved storage prior to releasing any classified material to a contractor.

DCSA verifies the PCLs in connection with granting or maintaining the FCL and ensures Key Management Personnel, including the SMO, the Insider Threat Program Security Official (ITPSO) 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.

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 DCSA Industrial Security Representative (ISRep) 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 DCSA, 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 KMP PCLs. 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 reviews.

Privity of Contract

Some contracts entail a 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 subcontractor. 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

Activity 1

Which of the following prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information?

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

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

Activity 2

Which of the following specifies DOD publications that implement the NISP and provide uniform policies and procedures for acquisition, including contractual security requirements?

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

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

Activity 3

Which of the following states that contracts classified as Confidential, Secret, or Top Secret must incorporate the Security Requirements statements?

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

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

Activity 4

Which of the following ensures DD Form 254 and the FAR Security Requirements clause is incorporated in the contract?

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

- ○ GCA
- ○ Contractor

Activity 5

Which of the following provides on-going security classification guidance throughout the contract performance period?

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

- ○ GCA
- ○ Contractor

Activity 6

Which of the following establishes and implements facility procedures in accordance with the NISPOM and DD Form 441?

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

- ○ GCA
- ○ Contractor

Activity 7

Which of the following submits the Registration for Scientific and Technical Information Services, DD Form 1540, if DTIC use is required for contract performance?

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

- ○ GCA
- ○ Contractor

Activity 8

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

Select all that apply. Then 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 clearances for all employees
- ☐ Comply with security requirements in the Contract Security Classification Specification

Activity 9

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

Select all that apply. Then 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 lesson “Security Requirements and Guidance.”

Lesson 4: Contract Administration and Security

Introduction

Objectives

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

Here are the lesson objectives:

- Describe the phases of contract administration and the impact of security requirements in the contracting process
  - Describe the activities in the contracting process phases
  - Explain the considerations and impact of security requirements during the contracting process phases
- Describe the purpose of the security-related contractual documents: DD Form 254, DD Form 441, SF 328
- Explain the relationship of the SOW or PWS to DD Form 254
  - Describe the purpose of the Statement of Work
  - Describe 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
    - Identify candidate countermeasures and sub-countermeasures
- 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 an 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 clearance by submitting a sponsorship letter to DCSA via the DCSA system of record for NISP, which will then allow the contractor to bid on the contract.

Pre-Solicitation: Step 1

The Pre-Solicitation stage has two major steps: Requirements Definition and the Acquisition Strategy.

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 acquisition planning.

- 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 includes sealed bid as defined in FAR 6.401 or contracting by negotiation defined FAR 15 in addition to FAR Part 8.4 Federal Supply Schedules, Part 13 Simplified Acquisition Procedures, Part 14 Sealed Bidding, Part 15 Contracting by Negotiation and Government Purchase Cards.

Pre-Solicitation: Step 2

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
- Source Selection Procedures of how the proposals will be evaluated

FAR 7.105 describes the contents of written acquisition plans for agencies. 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, or RFP, Request for Quote, or RFQ, and Invitation for Bid, or IFB.

Acquisitions over the simplified acquisition threshold, use the Request for Proposal, or 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: Step 1

The Source Selection Stage is required for all best-value, negotiated, competitive acquisitions under FAR Part 15. Evaluation criteria and source selection is also found in Parts 8.4 and 13.

There are two steps in the stage: 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.

Source Selection: Step 2

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.

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.gov
- 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, and conducting the post-award orientation meeting. 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.

DCSA oversees contractor compliance with the NISPOM when the classified work is performed at a cleared contractor facility. The SMO is ultimately responsible for the facilities operations while the FSO is responsible for implementing 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 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 DCSA 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 PWS or SOW. 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 lifecycle, 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 and DD Form 254

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. Block 1 addresses the FCL and safeguarding requirement; provides the contractor with specific clearance and access requirements for contracts requiring access to or creating classified information. 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.

Contract Security Classification Specification

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 18 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 as needed to authorize additional retention of classified information. The revised DD Form 254 is issued whenever there are changes to any classification guidance previously provided.

Contract Security Classification Specification

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.

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 for all companies cleared in the NISP. 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, the Certificate Pertaining to Foreign Interests is required. It must be submitted to DCSA 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-subsidiary 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. The work statements define the security level and mirror information found in more detail within the DD Form 254. 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 a work statement and a DD Form 254 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. It also defines the hours the contractor will work on project and the employees' hourly rates. 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 Quality Assurance Surveillance Plan (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. 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 approach is not without risk, but risk is shifted to the Government when using an SOW. 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

Activity 1

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

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

- ○ Pre-Award
- ○ Post-Award
- ○ Contract Management
- ○ Closeout

Activity 2

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

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

- ○ Pre-Award
- ○ Post-Award
- ○ Contract Management
- ○ Closeout

Activity 3

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

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

- ○ Pre-Award
- ○ Post-Award
- ○ Contract Management
- ○ Closeout

Activity 4

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

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

- ○ Pre-Award
- ○ Post-Award
- ○ Contract Management
- ○ Closeout

Activity 5

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

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

- ○ True
- ○ False

Activity 6

DCSA is involved with the contractor FCL process once the company is sponsored for an FCL.

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

- ○ True
- ○ False

Activity 7

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.

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

- ○ True
- ○ False

Activity 8

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

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

- ○ DD Form 254
- ○ DD Form 441
- ○ SF 328

Activity 9

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

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

- ○ DD Form 254
- ○ DD Form 441
- ○ SF 328

Activity 10

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

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

- ○ DD Form 254
- ○ DD Form 441
- ○ SF 328

Activity 11

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.

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

- ○ Performance Work Statement
- ○ Statement of Work

Activity 12

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

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

- ○ Performance Work Statement
- ○ Statement of Work

Activity 13

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

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

- ○ Performance Work Statement
- ○ Statement of Work

Activity 14

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 Specification
- ○ Performance Work Statement
- ○ Statement of Work

Conclusion

Lesson Summary

You have completed the lesson “Contract Administration and Security.”

Lesson 5: Course Conclusion

Course Conclusion

Course Summary

In this course, you learned about the DOD acquisition framework, the important role of the NISP for contracts requiring access to classified information, and the process for moving an acquisition through the system. 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 Performance Work Statement (PWS) and the Statement of Work (SOW) that are part of the solicitation package and awarded contract.

Lesson Review

Here is a list of the lessons in the course:

- Lesson 1: Course Introduction
- Lesson 2: DOD Acquisition Framework and Security Requirements
- Lesson 3: Security Requirements and Guidance
- Lesson 4: Contract Administration and Security
- Lesson 5: Course Conclusion

Lesson Summary

Congratulations! You have completed the *Acquisitions and Contracting Basics* course.

You should now be able to perform all of the listed activities.

- Identify the pathways in the acquisition framework
- Describe the role of security professionals in the DOD acquisition framework
- Recognize the importance of planning for security across the acquisition process and during the contracting process
- Describe the phases of contract administration and the impact of security requirements in the contracting process
- Describe the purpose of security-related contractual documents
- Explain 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. Please use the Security Training, Education, and Professionalization Portal (STEPP) system to access the online exam.

Appendix A: Answer Key

Lesson 2 Review

Activity 1

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)
- ◉ Technology Maturation & Risk Reduction (TMRR) (correct response)
- ○ Engineering & Manufacturing Development (EMD)
- ○ Production & Deployment (P&D)
- ○ Operations & Support (O&S)

***Feedback**: During the Technology Maturation & Risk Reduction (TMRR) Phase, the Capability Design Document (CDD) is approved with system-specific requirements, the Request for Proposal (RFP) is released to industry, and technical design and analyses begins.*

Activity 2

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)
- ○ Technology Maturation & Risk Reduction (TMRR)
- ○ Engineering & Manufacturing Development (EMD)
- ◉ Production & Deployment (P&D) (correct response)
- ○ Operations & Support (O&S)

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

Activity 3

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)
- ○ Technology Maturation & Risk Reduction (TMRR)
- ◉ Engineering & Manufacturing Development (EMD) (correct response)
- ○ Production & Deployment (P&D)
- ○ Operations & Support (O&S)

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

Activity 4

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

***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.*

Activity 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)
- ○ Technology Maturation & Risk Reduction (TMRR)
- ○ Engineering & Manufacturing Development (EMD)
- ○ Production & Deployment (P&D)
- ⦿ Operations & Support (O&S) (correct response)

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

Activity 6

The 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.*

Activity 7

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

- ⦿ True (correct response)
- ○ False

***Feedback**: The Cognizant Security Agencies (CSAs) establish industrial security programs and provide security oversight to include monitoring cleared companies and determining eligibility for access to classified information.*

Activity 8

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 Materiel Solution Analysis Phase.*

Activity 9

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

- ○ Contracting Officer's Representative (COR)
- ⦿ Contracting Officer (correct response)
- ○ Defense Counterintelligence and Security Agency (DCSA)
- ○ Contractor

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

Activity 10

Issues subcontracts with the DD Form 254.

- ○ Contracting Officer's Representative (COR)
- ○ Contracting Officer
- ○ Defense Counterintelligence and Security Agency (DCSA)
- ⦿ Contractor (correct response)

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

Activity 11

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 Counterintelligence and Security Agency (DCSA)
- ○ Contractor

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

Activity 12

Conducts security reviews on contractors and coordinates with the appropriate DOD representatives and Security Specialists on damage assessments.

- ○ Contracting Officer's Representative (COR)
- ○ Contracting Officer
- ⦿ Defense Counterintelligence and Security Agency (DCSA) (correct response)
- ○ Contractor

***Feedback**: The Defense Counterintelligence and Security Agency (DCSA) conducts security reviews 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.*

Lesson 3 Review

Activity 1

Which of the following 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.*

Activity 2

Which of the following specifies DOD publications that implement the NISP and provide 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.*

Activity 3

Which of the following 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.*

Activity 4

Which of the following ensures DD Form 254 and the FAR Security Requirements clause is incorporated in the contract?

- ⦿ GCA (correct response)
- ○ Contractor

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

Activity 5

Which of the following provides on-going security classification guidance throughout the contract performance period?

- ⦿ GCA (correct response)
- ○ Contractor

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

Activity 6

Which of the following establishes and implements facility procedures in accordance with the NISPOM and DD Form 441?

- ○ 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.*

Activity 7

Which of the following submits the Registration for Scientific and Technical Information Services, DD Form 1540, if DTIC use is required for contract performance?

- ○ 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.*

Activity 8

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 clearances 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.*

Activity 9

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.*

Lesson 4 Review

Activity 1

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

- ○ Pre-Award
- ○ Post-Award
- ◉ Contract Management (correct response)
- ○ Closeout

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

Activity 2

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

- ○ Pre-Award
- ◉ Post-Award (correct response)
- ○ Contract Management
- ○ Closeout

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

Activity 3

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

- ◉ Pre-Award (correct response)
- ○ Post-Award
- ○ Contract Management
- ○ Closeout

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

Activity 4

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

- ○ Pre-Award
- ○ Post-Award
- ○ Contract Management
- ⦿ Closeout (correct response)

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

Activity 5

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.*

Activity 6

DCSA is involved with the contractor FCL process once the company is sponsored for an FCL.

- ⦿ True (correct response)
- ○ False

***Feedback**: DCSA is involved with the contractor FCL process once the company is sponsored for an FCL. DCSA does not provide input on the security requirements.*

Activity 7

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.*

Activity 8

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.*

Activity 9

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.*

Activity 10

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.*

Activity 11

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.*

Activity 12

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.*

Activity 13

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.*

Activity 14

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

***Feedback**: The statement is from a DD Form 254 - Contract Security Classification Specification, Block 13: Security.*