Glossary

Acquisition and Contracting Basics

Access: The ability and opportunity to gain knowledge of classified information.

Acquisition Life Cycle: The management process by which the Department of Defense provides effective, affordable, and timely systems to the users. It consists of phases containing major activities and associated decision points, during which a system goes through research, development, test, and evaluation (RDT&E); production; fielding or deployment; sustainment; and disposal. Currently, there are five phases, three milestone decisions, and four decision points.

Acquisition Program: A directed, funded effort that provides a new, improved, or continuing materiel, weapon, or information system or service capability in response to an approved need. Acquisition programs are divided into categories that are established to facilitate decentralized decision making, execution, and compliance with statutory requirements.

Acquisition: The conceptualization, initiation, design, development, test, contracting, production, deployment, logistics support (LS), modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in, or in support of, military missions.

Adversary: An individual, group, organization, or Government that must be denied Critical Program Information (CPI). Synonymous with competitor/enemy.

Alternative Systems Review (ASR): A multi-disciplined technical review to ensure that requirements agree with the customers' needs and expectations and that the system under review can proceed into the Technology Maturation and Risk Reduction (TMRR) phase. The ASR should be completed prior to Milestone A.

Analysis of Alternatives (AoA): Assessment of potential materiel solutions to satisfy the capability need documented in the approved Initial Capabilities Document (ICD). It focuses on identification and analysis of alternatives, Measures of Effectiveness (MOE), cost, schedule, concepts of operations, and overall risk, including the sensitivity of each alternative to possible changes in key assumptions or variables.

Analysis of Alternatives (AoA) Study Plan: Based on the AoA Study Guidance, the AoA Study Plan establishes a roadmap of how the analysis must proceed, who is responsible for the different elements, and why they are doing them. The Study Plan is a "living document" and must be updated throughout the AoA effort to reflect new information and changing study perceptions and direction.

Capability Design Document (CDD): A CDD (includes the Information System (IS) CDD variant) specifies capability requirements in terms of developmental Key Performance Parameters (KPPs), Key System Attributes (KSAs), Additional Performance Attributes (APAs), and other related information necessary to support development of one or more increments of a materiel capability solution.

Certificate Pertaining to Foreign Interests – SF 328: Is required when cleared company's path might lead to effective ownership or control by a foreign interest. It is to prevent unauthorized access to classified information and operations and management that may adversely affect the performance of classified contracts.

Classification Management: Consists of three elements. What needs to be protected, how much protection is required and declassification of National Security information. It is a joint responsibility between the contractor and the U. S. government (GCA).

Classified Contract: Any contract requiring access to classified information by a contractor in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.) The requirements prescribed for a "classified contract" also are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other GCA program or project which requires access to classified information by a contractor.

Classified Information: Official information that has been determined, pursuant to Executive Order 12958 or any predecessor order, or pursuant to the Atomic Energy Act of 1954, to require protection against unauthorized disclosure in the interest of national security which has been designated.

Cleared Contractors: All contractor employees granted PCLs and all employees being processed for PCLs.

Cognizant Security Agencies (CSAs): Agencies of the Executive Branch that have been authorized by Executive Order 12829 to establish an industrial security program to safeguard classified information under the jurisdiction of these agencies when disclosed or released to U.S. Industry. These agencies are: The Department of Defense, Office of the Director of National Intelligence, Department of Energy, Nuclear Regulatory Commission, and Department of Homeland Security.

Cognizant Security Office (CSO): The organizational entity delegated by the head of a CSA to administer industrial security on behalf of the CSA.

Commercial and Government Entity (CAGE) Code: A five position code that identifies companies doing or wishing to do business with the Federal Government. The first and fifth positions in the code must be numeric. The third and fourth positions may be any mixture of alpha/numeric excluding I and O. The code is used to support a variety of mechanized systems throughout the Government.

Communications Security (COMSEC): Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. government relating to national security and to ensure the authenticity of such communications.

Compromise: An unauthorized disclosure of information.

Contract Award: Requires completion of final evaluations and approval of the required clearance documentation and GCA notifies the contractor of the award.

Contract Closeout: During this phase the Contracting Officer must ensure that the work conforms to the requirements in the SOW or PWS. Any deficiencies must be resolved before final payment is made. All classified material must be returned to the GCA or destroyed.

Contract Management: In the Contract Management phase, the contractor provides the agreed-upon product or service. The GCA works with the FSO and ISSM to monitor and mitigate threats and vulnerabilities.

Contract Security Classification Specification – DD Form 254: DD Form 254 provides to the cleared contractor, or cleared subcontractor the security requirements and the classification guidance that are necessary to perform on a specific classified contract.

Contracting Officer: Has the authority to enter into, administer, and terminate contracts. As well as ensures all contract actions comply with appropriate laws, executive orders, regulations, and other applicable procedures and approvals.

Contracting Officer's Representative (COR): Determines the need for contractor access to classified information, verifies the FCL and communicates the security requirements during the procurement process and contract performance.

Contractor: Any industrial, educational, commercial, or other entity that has been granted an FCL by a CSA.

Critical Design Review (CDR): A multi-disciplined technical review to assess design maturity, design build-to or code-to documentation and remaining risks, and establish

the initial product baseline. It is used to determine whether the system design is ready to to begin developmental prototype hardware fabrication and/or software coding with acceptable risk.

Critical Program Information (CPI): Elements or components of a research, development, and acquisition (RDA) program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability.

Criticality Analysis (CA): Procedure by which each potential failure mode is ranked according to the combined influence of severity and probability of occurrence.

DD Form 254: Contract Security Classification Specification

DD Form 441: DoD Security Agreement

DD Form 1540: Registration for Scientific and Technical Information Services

Defense Security Service (DSS): The Defense Security Service (DSS) is an agency of the Department of Defense (DoD) located in Quantico, Virginia with field offices throughout the United States. The Under Secretary of Defense for Intelligence provides authority, direction and control over DSS. DSS provides the military services, Defense Agencies, 30 federal agencies and approximately 13,500 cleared contractor facilities with security support services. DSS is the CSO for most DoD classified contracts.

DSS supports the National Security and the warfighter, secures the nation's technological base, and oversees the protection of U. S. and foreign classified information in the hands of industry. DSS conducts security vulnerability assessments and coordinates with the appropriate DoD representatives and Security Specialists on damage assessments in case of contractor loss, compromise, or suspected compromise of classified information

Defense Security Service, Center for Development of Security Excellence (CDSE): The Center for Development of Security Excellence is responsible for providing security education and training to DoD and other U.S. Government personnel, DoD contractors, and sponsored representatives of foreign governments.

Defense Security Service, Foreign Ownership Control or Influence (FOCI) Office: This office within the Defense Security Service works with the local IS Rep to resolve issues that arise when a cleared facility or a facility being processed for a facility clearance is subject to foreign ownership, control or influence.

Defense Security Service, Industrial Security Representative (IS Rep): Local representative from the Defense Security Service that provides advice and assistance on security matters and with establishing your security program to ensure your facility is in compliance with the NISP.

Defense Security Service, Information Systems Security Professional (ISSP): Local representative from the Defense Security Service, Office of Designated Approving Authority (ODAA) that provides advice and assistance visits to improve the security posture with regard to Information Systems and help facilitate the process of getting your information systems accredited to process classified information.

Defense Technical Information Center (DTIC): The repository for research and engineering information for the Department of Defense (DoD). Its Suite of Services is available to DoD personnel, defense contractors, Federal Government personnel and contractors, and selected academic institutions. The general public can also access unclassified, unlimited information, including many full-text downloadable documents, through the public DTIC web site.

Development RFP Release Decision: The point at which planning for development is complete and a decision is made to release a Request for Proposal (RFP).

Developmental Test and Evaluation (DT&E): Any testing used to assist in the development and maturation of products, product elements, or manufacturing or support processes. Any engineering-type test used to verify status of technical progress, verify that design risks are minimized, substantiate achievement of contract technical performance, and certify readiness for initial operational testing. Developmental tests generally require instrumentation and measurements and are accomplished by engineers, technicians, or soldier operator-maintainer test personnel in a controlled environment to facilitate failure analysis.

Director of National Intelligence (DNI): Retains authority over access to intelligence sources and methods.

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.

DoD Security Agreement – DD Form 441: Is entered into between a contractor who will have access to classified information, and the DoD in order to preserve and maintain the security of the U.S. through the prevention of unauthorized disclosure of classified information. It also defines what the contractor agrees to do and what the Government agrees to do regarding security responsibilities as part of the FCL process.

DoD Security Specialist: Also called Activity Security Managers act as the GCA representatives to the NISP and serve as resident security subject matter experts (SMEs).They also maintain security cognizance over all activity information, personnel, information systems, physical security and industrial security.

Eligibility: A DoD Consolidated Adjudication facility (DoD CAF) has made an adjudicative determination of member's Personnel Security Investigation (PSI) and that member may have access to classified information equal to the level of their adjudicated investigation.

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

Executive Order (EO): An order issued by the President to create a policy and regulate its administration within the Executive Branch.

Facility: A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined herein.) For the purposes of industrial security, the term does not include Government installations.

Facility (Security) Clearance (FCL): An Administrative determination that, from a security viewpoint, a company is eligible for access to classified information of a certain category (and all lower categories).

Facility Security Officer (FSO): A U.S. citizen employee, appointed by a contractor who will supervise and direct security measures necessary for implementing the NISPOM and other Federal requirements for classified information.

FAR Clause: Applies to the extent that the contract involves access to information classified as Confidential, Secret, or Top Secret. The clause further states that the contractor shall comply with the Security Agreement (DD Form 441, including the NISPOM and any revisions to the manual, notice of which has been furnished to the contractor.

Federal Acquisition Regulation (FAR): Provides uniform policies and procedures for acquisition as well as calls for the implementation of the NISPOM and ISR.

Foreign Interest: Any government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than

the United States or its territories, and any person who is not a citizen or national of the United States.

Foreign Ownership, Control, or Influence (FOCI): Whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable, to direct or decide matters affecting the management or operations of a company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

Full Rate Production: The second effort part of the Production and Deployment (P&D) phase as defined and established by DoDI 5000.02 after Low-Rate Initial Production (LRIP) and following a successful Full-Rate Production Decision Review (FRPDR).

Functional Configuration Audit (FCA): Verifies that all item or subsystem requirements established in the functional and allocated baselines, specifications, and test plans have been tested successfully, and corrective action has been initiated, as necessary.

Government Contracting Activity (GCAs): An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.

Industrial Security: That portion of information security concerned with the protection of classified information in the custody of U.S. industry.

Industrial Security Facilities Database (ISFD): System of record for facility clearance information.

Industrial Security Letters (ISLs): Documents that provide detailed operational guidance and notification of changes to or clarification of existing policies or requirements to the NISPOM.

Information Security: The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order.

Information System Security Manager (ISSM): An individual appointed by a contractor with oversight responsibility for the development, implementation, and evaluation of the facility's information system security program. The ISSM must be trained to a level commensurate with the complexity of the facility's information systems.

Information System Security Officer (ISSO): ISSOs may be appointed by the ISSM in facilities with multiple accredited information systems. The ISSM will determine the responsibilities to be assigned to the ISSO in accordance with NISPOM Chapter 8.

Initial Capabilities Document (ICD): Documents one or more new capability requirements and associated capability gaps. The ICD also documents the intent to partially or wholly address identified capability gap(s) with a non-materiel solution, materiel solution, or some combination of the two.

Initial Operational Test and Evaluation (IOT&E): Dedicated Operational Test and Evaluation (OT&E) conducted on production or production representative articles, to determine whether systems are operationally effective and suitable to support a Full-Rate Production (FRP) decision. The term IOT&E is normally associated with programs on the Director, Operational Test and Evaluation Oversight List.

Key Management Personnel (KMP): Senior management identified in a facility that require an eligibility determination in order for a facility to be granted a facility clearance.

Key Performance Parameters (KPPs): Performance attribute of a system considered critical or essential to the development of an effective military capability. KPPs are contained in the Capability Development Document (CDD) and the Capability Production Document (CPD) and are included verbatim in the Acquisition Program Baseline (APB).

Key System Attributes (KSAs): Performance attribute of a system considered important to achieving a balanced solution/approach to a system, but not critical enough to be designated as a Key Performance Parameter (KPP). KSAs must be measurable, testable, and support efficient and effective Test and Evaluation (T&E).

Life Cycle Sustainment: Translates force provider capability and performance requirements into tailored product support to achieve specified and evolving life cycle product support availability, reliability, and affordability parameters. Life cycle sustainment considerations include supply; maintenance; transportation; sustainment engineering; data management; configuration management; human systems integration (HSI); environment, safety (including explosives), and occupational health; protection of critical program information and anti-tamper provisions, supportability, and interoperability.

Life Cycle Sustainment Plan (LCSP): Initially prepared for Milestone A and updated for the Development Request For Proposal (RFP) Release Decision Point, Milestone B, Milestone C, Full-Rate Production Decision Review (FRPDR) and at least every 5 years after a system's Initial Operational Capability (IOC).

Lowest Price and Technically Acceptable: Source Selection Process appropriate when best value is expected to result from selection of a technically acceptable proposal with the lowest evaluated price.

Low-Rate Initial Production (LRIP): The first part of the Production and Deployment (P&D) phase. LRIP is intended to result in completion of manufacturing development in order to ensure adequate and efficient manufacturing capability and to produce the minimum quantity necessary to provide production or production-representative articles for Initial Operational Test and Evaluation (IOT&E).

Materiel Development Decision (MDD): A review that is the formal entry point into the acquisition process and is mandatory for all programs. A successful MDD may approve entry into the acquisition management system at any point consistent with phase-specific and statutory requirements but will normally be followed by a Materiel Solution Analysis (MSA) phase.

Materiel Solution Analysis (MSA): Conduct the analysis and other activities needed to choose the concept for the product that will be acquired. 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.

Milestone (MS): In the context of scheduling, a specific definable accomplishment in the contract network that is recognizable at a particular point in time.

Milestone Decision Authority (MDA): Designated individual with overall responsibility for a program. The MDA shall have the authority to approve entry of an acquisition program into the next phase of the acquisition process and shall be accountable for cost, schedule, and performance reporting to higher authority, including congressional reporting.

National Industrial Security Program (NISP): The National Industrial Security Program (NISP) was established by Executive Order 12829 for the protection of classified information released or disclosed to industry in connection with classified contracts. The NISP applies standards for the protection of classified information released or disclosed to contractors of all federal executive branch departments and agencies. Requirements of the NISP are stated in the National Industrial Security Program Operating Manual (NISPOM), (DoD 5220.22-M).

National Industrial Security Program Operating Manual (NISPOM): A manual issued in accordance with the National Industrial Security Program that prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified of classified information.

National Interest Determination (NID): Is a written statement by the Government Contracting Activity or GCA, affirming that the release of proscribed information to the company will not harm the National Security interests of the U.S.

NISP Contract Classification System (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.

Operations & Support (O&S): Phase that executes the product support strategy, satisfy materiel readiness and operational support performance requirements, and sustain the system over its life cycle (to include disposal). Concerns center on sustainment of the fielded system as well as disposal at end-of-life.

Original Classification Authority (OCA): An individual authorized in writing, either by the United States (U.S.) President, or by agency heads or other officials designated by the President, to classify information in the first instance. OCAs must receive training to perform this duty.

Performance Work Statement (PWS): States the work in terms of outcomes or results, rather than methods of performance. It defines measurable performance standards and financial incentives.

Personnel (Security) Clearance (PCL): An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

Physical Configuration Audit (PCA): Physical examination of the actual configuration of the item being produced. It verifies that the related design documentation matches the item as specified in the contract. The system product baseline if finalized and validated at the PCA.

Post-Award: During this phase, the government and the contractor meet and prepare to implement the contract. The program stakeholders come together to review the contract performance requirements and security issues.

Pre-Award: During this phase acquisition planning, issuing the solicitation, and source selection occur. The solicitation is released with the FAR Security Requirements Clause for classified contracts.

Pre-Award Objective: Is to award the contract to the proposal that represents the best value to the Government.

Pre-Solicitation: Discusses technical and other problems connected with a proposed procurement.

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 and perform an initial Criticality Analysis (CA) based on mission threats and system functions.

Preliminary Design Review (PDR): A design review that assesses the maturity of the preliminary design supported by the results of requirements trades, prototyping, and critical technology demonstrations. The PDR establishes the allocated baseline (hardware, software, human/support systems) and underlying architectures to ensure the system under review has a reasonable expectation of satisfying the requirements within the currently allocated budget and schedule, and confirms that the system under review is ready to proceed into detailed design (development of build-to drawings, software code-to documentation and other tasks) with acceptable risk.

Prime Contractor: Is responsible for disclosing classified information to cleared subcontractors.

Privity of Contract: Refers to the direct relationship that exists between contracting parties.

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

Production Readiness Review (PRR): A formal examination of a program to determine if the design is ready for production and if the prime contractor and major subcontractors have accomplished adequate production planning without incurring unacceptable risks that will breach thresholds of schedule, performance, cost, or other established criteria. PRRs are normally performed as a series of reviews toward the end of Engineering and Manufacturing Development (EMD) phase.

Program Manager (PM): Ensures resources are programmed and necessary IP deliverables and associated license rights, tools, equipment, and facilities are acquired to support each of the levels of maintenance that will provide product support and establishes necessary organic depot maintenance capability in compliance with statute and the LCSP.

Quality Assurance Surveillance Plan (QASP): The document government personnel use to assess contractor performance. The QASP identifies what is going to be inspected, the inspection process, and who will do the inspecting.

Registration for Scientific and Technical Information Services - DD Form 1540: Used to validate an individual's required affiliation with a DoD organization.

Request for Proposal (RFP): Is a formal negotiated solicitation that results in a formal contract award.

Request for Quote (RFQ): A solicitation used in negotiated acquisition to communicate government requirements to prospective contractors and to solicit a

quotation. A response to an RFQ is not an offer; however, it is informational in character.

Research and Development (R&D): Research and Development (R&D) category 01 under Major Force Program (MFP) 6 (R&D) of the Future Years Defense Program (FYDP). Includes all scientific study and experimentation directed toward increasing knowledge and understanding in those fields of the physical, engineering, environmental, and life sciences related to long-term national security needs.

Security Training Education and Professionalization Portal (STEPP): The learning management system used by the Center for Development of Security Excellence (CDSE). STEPP is where the list of courses is maintained and where student information and course transcripts are maintained.

SF 328: Certificate Pertaining to Foreign Interests

Solicitation: This stage is concerned with contract formulation, including the contract form contract clauses, work statement, specifications delivery schedule, and payment terms.

Special Access Program (SAP): Any program that is established to control access, distribution, and to provide protection for particularly sensitive classified information beyond that normally required for TOP SECRET, SECRET, or CONFIDENTIAL information. A Special Access Program can be created or continued only as authorized by a senior agency official delegated such authority pursuant to the NISPOM.

Statement of Work (SOW): Designed to describe not only what is to be done but also how it is to be done.

Subject Matter Expert (SME): An expert in a particular field who contributes or verifies the accuracy of specific information needed by the project team.

Sustainment: Programs with Critical Program Information (CPI) require continued evaluation and monitoring as protection and threat / vulnerability / countermeasures may have to continue to evolve.

System Acquisition: Update criticality assessment, risk, threat and mitigation as required and ensure all Critical Program Information (CPI) and mission-critical functions are identified and associated countermeasures applied.

System Functional Review (SFR): A multi-disciplined technical review to ensure that the system's functional baseline is established and has a reasonable expectation of satisfying the requirements of the Initial Capabilities Document (ICD) or draft Capability Development Document (CDD) within the currently allocated

budget and schedule. It completes the process of defining the items or elements below system level.

Systems Security Engineering (SSE): Is performed by a variety of professionals from government and industry to ensure a comprehensive analysis of system technology, hardware, software, firmware, and information.

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

Test and Evaluation (T&E): Process by which a system or components are exercised and results analyzed to provide performance-related information. The information has many uses including risk identification and risk mitigation and empirical data to validate models and simulations.

Tradeoff: Source Selection Process allows for a tradeoff between non-cost factors and cost/price and allows the Government to accept other than the lowest priced proposal or other than the highest technically rated proposal to achieve a best-value contract award.