Glossary

Course: Introduction to Industrial Security

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

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.

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.

Administrative Contracting Officer (ACO): The ACO administers the day-to-day activities following the contract award. The ACO may not have official Contracting Officer status but may be a delegate of the Contracting Officer.

Administrative Inquiry: A broad overview of the investigation that is underway. This is the second step in reporting a security violation.

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.

Arms, Ammunition and Explosives (AA&E): Program that provides guidance regarding the safety of arms, ammunitions and explosives.

Assessment and Evaluations (A&E): Monitors contractors for changes impacting their Facility Clearance (FCL) and analyses, reports and certifies data for Personnel Security Investigations (PSIs).

Authorizing Official (AO): The Authorizing Official (AO) is the senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions,

image, or reputation), organizational assets, individuals, other organizations, and national security.

Authorizing Official Designated Representative (AODR): An individual designated by the Authorizing Official (AO) to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and national security.

Classification: 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.

Classified Visit: A visit during which a visitor will require, or is expected to require, access to classified information.

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

Cognizant Security Agencies (CSAs): Agencies of the Executive Branch that were authorized by Executive Order (EO) 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. Those agencies are: The Department of Defense, Office of the Director of National Intelligence, Department of Energy, and the Nuclear Regulatory Commission. EO 13691 established the Department of Homeland Security as a CSA.

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

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.

Company: A generic and comprehensive term that may include sole proprietorships, individuals, partnerships, corporations, societies, associations, and organizations usually established and operating to carry out a commercial, industrial, or other legitimate business, enterprise, or undertaking.

Compromise: An unauthorized disclosure of information.

CONFIDENTIAL: The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

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

Contracting Officer (CO): The CO 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): The 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 Nuclear Weapons Design Information (CNWDI):** A DoD category of TOP SECRET RD or SECRET RD that reveals the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munition, or test device.

Controlled Unclassified Information (CUI): Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or

permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.

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.

Cyber Security: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication including information contained therein, to ensure its availability, integrity, authentication confidentiality and non-repudiation.

Defense Federal Acquisition Regulation Supplement (DFARS): The DFARS implements and supplements the Federal Acquisition Regulation (FAR), and is administered by the Department of Defense (DoD). The DFARS should be read in conjunction with the primary set of rules in the FAR.

Defense Information System for Security (DISS): DISS will replace the Joint Personnel Adjudication System (JPAS). DISS consists of two main components, the Case Adjudication Tracking System (CATS) and the DISS Portal which will replace the Joint Clearance and Access Verification System (JCAVS).

Defense Security Service (DSS): The DSS is an agency of the 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, 31 federal agencies and approximately 13,500 cleared contractor facilities with security support services.DSS supports national security and the service members, secures the nation's technological base, and oversees the protection of U.S. and foreign classified information in the hands of industry. DSS accomplishes this mission by clearing industrial facilities, accrediting information systems, facilitating the personnel security clearance process, delivering security education, training, and certification and providing information technology services that support the industrial and personnel security missions of DoD and its partner agencies.

Defense Security Service (DSS), Center for Development of Security Excellence (CDSE): The Center for Development of Security Excellence (CDSE) is a nationally accredited, award-winning directorate within the DSS. CDSE provides security education, training, and certification products and services for the DoD and industry.

Defense Security Service (DSS), Counterintelligence (CI) Office: Office within the Defense Security Service that provides counterintelligence support to DSS through CI reviews, assessments, analysis, and reports.

Defense Security Service (DSS), Counterintelligence Special Agent (CISA): Assists FSOs in identifying potential threats to U.S. technology and developing CI awareness and reporting by company employees.

Defense Security Service (DSS), Facility Clearance Branch (FCB): The DSS FCB processes contractors for FCLs based upon procurement need, issues FCLs, and monitors the contractor's continued eligibility in the NISP.

Defense Security Service (DSS), Field Office Chief (FOC): Manages implementation of NISP and AA&E programs. Ensures effective counterintelligence support to cleared facilities and government contracting activities throughout area of responsibility. Oversees the conduct of security vulnerability assessments by IS Reps. Manages office budget, vehicle utilization, and other property.

Defense Security Service (DSS), Foreign Ownership Control or Influence (FOCI) Operations Division: This office within the DSS works with the local Industrial Security Representative (IS Rep) to resolve issues that arise when a cleared facility or a facility being processed for a FCL is subject to FOCI.

Defense Security Service (DSS), Industrial Security Field Operations (ISFO): Provides oversight and conducts Security Vulnerability Assessments (SVA) for approximately 13,500 cleared contractor facilities. They maintain industrial security field offices all over the country.

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

Defense Security Service (DSS), Information Systems Security Professional/Security Control Assessor (ISSP/SCA): The ISSP/SCA performs oversight of a contractor's information system processing classified information and provides an authorization decision recommendation to the Authorizing Official (AO).

Defense Security Service (DSS), National Industrial Security Program Authorization Office (NAO): Office within the DSS that facilitates the Assessment and Authorization (A&A) process for classified information systems at cleared contractor facilities.

Defense Security Service (DSS), Personnel Security Management Office for Industry (PSMO-I): An office within the DSS that processes requests for, and other actions related to PCLs for personnel from facilities participating in the NISP.

Defense Security Service (DSS), Special Programs: Manages the security oversight function of DSS' direct and indirect support to the Special Access Program (SAP) community.

Department of Defense (DoD): The DoD is an executive branch department of the federal government of the U. S. charged with coordinating and supervising all agencies and functions of the government concerned directly with national security and the United States Armed Forces. The major elements of these forces are the Army, Navy, Marine Corps, and Air Force.

Department of Defense 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.

Department of Defense Security Agreement – DD 441: A DoD Security Agreement that 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.

Department of Defense System of Record: This is currently JPAS. In the future JPAS will be replaced by the Defense Information System for Security (DISS).

Department of Energy (DOE): The DOE is an executive department of the federal government concerned with the United States' policies regarding energy and safety in handling nuclear material.

Department of Homeland Security (DHS): The DHS is an executive department of the federal government that was established in response to the aftermath of September 11, 2001. Their primary objective is to protect U.S. citizens and interests from terrorist attacks.

Department of Defense (DoD) Security Specialist: Also called Activity Security Managers that 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): Contains the rules for government acquisition. These rules provide instruction, forms and guidance on government contracting.

For Official Use Only (FOUO): FOUO is a security designation used as a handling instruction for Controlled Unclassified Information (CUI) which may be exempt from release under exemptions two through nine of the Freedom of Information Act (FOIA).

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): A state in which a contracting agency may find itself in, that may impede its ability to be granted a Facility Security

Clearance. The agency will be considered under FOCI if a foreign entity has control, direct or indirect and whether or not exercised, over decisions that affect the management or operation of the organization

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.

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 Systems: An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information and textual material.

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): An Information System Security Officer (ISSO) is assigned by the ISSM when the facility has multiple authorized ISs in multiple facility organizations in which the ISSM has oversight responsibility for the multiple facilities, or when the technical complexity of the facility's IS program warrants the appointment.

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.

Insider Threat: The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information.

Insider Threat Program Senior Official (ITPSO): A U.S. citizen employee, appointed by a contractor who establishes and maintains a contractor insider threat program.

Intelligence: The product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information, that concerns one or more aspects of foreign nations or of areas of foreign operations, and that is immediately or potentially significant to military planning and operation

Intrusion Detection System (IDS): A device or software application that monitors a network or systems for malicious activity or policy violations.

Joint Personnel Access System (JPAS): The current DoD system of record. In the future JPAS will be replaced by the Defense Information System for Security (DISS).

Key Management Personnel (KMP): Key management personnel are Senior Management Officials (SMO) who have the authority to directly or indirectly plan and control business operations. KMPs require an eligibility determination before a facility is granted a FCL.

Material 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.

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.

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) – DoD 5200.22M: A manual issued in accordance with the NISP that prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information.

National Security Threat: An entity capable of aggression or harm to the United States.

Need-to-Know (NTK): A determination made by an authorized holder of classified information that a prospective recipient has a requirement for access to, knowledge, or

possession of the classified information to perform tasks or services essential to the fulfillment of a classified contract or program.

Nuclear Regulatory Commission: The NRC was created as an independent agency by Congress in 1974 to ensure the safe use of radioactive materials for beneficial civilian purposes while protecting people and the environment. The NRC regulates commercial nuclear power plants and other uses of nuclear materials, such as in nuclear medicine, through licensing, inspection and enforcement of its requirements.

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

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.

Personally Identifiable Information (PII): PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

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.

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.

Prime Contractor: The contractor who receives a prime contract from a GCA and is responsible for disclosing classified information to cleared subcontractors.

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.

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.

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.

SECRET: The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security.

Security Classification Guide (SCG): A document issued by an authorized original classifier that identifies the elements of information regarding a specific subject that must be classified and prescribes the level and duration of classified and appropriate declassification instructions. Classification guides for contractors are referenced in the Contract Security Classification Specification (DD Form 254) and provided by the GCA.

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.

Security Violation: A failure to comply with the policy and procedures established by the NISPOM that reasonably could result in the loss or compromise of classified information.

Security Vulnerability: All instances of non-compliance with the NISPOM that are not acute or critical vulnerabilities. Any weakness that can be exploited by an adversary to gain access to an asset. Vulnerabilities can result from, but are not limited to, the following: building characteristics; equipment properties; personal behavior; locations of people, equipment and buildings; or operational and personnel practices.

Security Vulnerability Assessment (SVA): A review of a contractor security program done by a Defense Security Service Industrial Security Representative. The SVA can be done individually or as a team.

Self-Inspection: The NISPOM requires all participants in the NISP to conduct their own self-inspections to include an insider threat self-assessment. The self-inspection requires a review of the Industrial Security Program and security procedures established within a company, and validate that they not only meet NISPOM requirements but are effectively implemented by cleared employees. Self-inspections should be tailored to the classified needs of the cleared company and are conducted to ensure the continued protection of national security.

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.

Standard Practice Procedures (SPP): A document(s) prepared by a contractor that implements the applicable requirements of the NISPOM for the contractor's operations and involvement with classified information at the contractor's facility.

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

Subcontractor: The contractor who receives a contract, or a portion of a contract from the Prime Contractor or from another subcontractor; and is responsible for disclosing classified information.

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

Suspicious Contact: Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country.

Suspicious Contact Reports (SCRs): A report of CI concern that likely represents efforts by an individual to obtain illegal or unauthorized access to classified information or technology.

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.

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.

Termination Contracting Officer (TCO): A TCO will negotiate the terms of termination of an existing contract with a government contractor, if the contract needs be terminated early, whether for convenience or cause.

TOP SECRET: The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

Unauthorized Disclosure: A communication or physical transfer of classified information to an unauthorized recipient.