Visits and Meetings in the NISP Glossary

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

CAGE Code: Commercial and Government Entity Code - a five position code that identifies contractors doing business with the Federal Government, NATO member nations, and other foreign governments and is used to support a variety of mechanized systems throughout the government and provides for a standardized method of identifying a given facility at a specific location.

Classification Guide: 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 are provided to contractors by the Contract Security Classification Specification)

Classified Contract: Any contract requiring access to classified information by a contractor or his or her employees in the performance of the contract. (A contract may be a classified contract even through 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 Government Contracting Activity programs or projects which require 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 Information Nondisclosure Agreement (Standard Form-SF 312):
An official authorized contract between an individual and the U.S. Government signed by the individual as a condition of access to classified information. This contractual agreement, which is signed prior to the individual's access, addresses the individual's responsibilities to protect classified information and the penalties for non-compliance.

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 a Personnel Security Clearance and all employees being processed for such a clearance.

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, Department of Energy, Central Intelligence Agency, and Nuclear Regulatory Commission.

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.

Compromise: An unauthorized disclosure of information.

CONFIDENTIAL: The classification level applied to information, the unauthorized disclosure of which reasonable could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

Contract Security Classification Specification (DD Form 254): This document provides the Prime Contractor or subcontractor with the security requirements and the classification guidance that is necessary to execute a classified contract.

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

Controlled Unclassified Information (CUI): A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification pursuant to Executive Order (EO) 13526, "Classified National Security Information," Reference (e), but is pertinent to the national interests of the U.S. or to the important interests of entities outside the Federal Government and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. NOTE: The designation Controlled Unclassified Information replaces the term Sensitive but Unclassified.

DD Form 254: Contract Security Classification Specification

DD Form 441 (Security Agreement): A Department of Defense (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.

Defense Information System for Security (DISS): The DoD system of record for contractor eligibility and access for personnel security clearances.

Defense Security Service (DSS): DSS is a DoD agency DoD headquartered 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, 25 federal agencies and approximately 12,000 cleared contractor facilities with security support services. DSS is the CSO for most DoD classified contracts.

DSS supports national security and the warfighter, secures the nation's technological base, and oversees the protection of US 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 and training, and providing information technology services that support the industrial and personnel security missions of DoD and its partner agencies.

Defense Security Service (DSS) Counterintelligence (CI) Directorate: This Directorate provides counterintelligence support through CI reviews, assessments, analysis, and reports.

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

Defense Security Service (DSS) Foreign Ownership Control or Influence (FOCI) Division: The FOCI Division, 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 (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.

Department of Defense Consolidated Adjudications Facility (DoD CAF): Responsible for all adjudicative functions.

Eligibility: An adjudicative determination made by the DoD CAF, based on a Personnel Security Investigation, that an individual may be granted access to classified information up to but not to exceed the level supported by the investigation.

Export Administration Regulations (EAR): The U.S. Department of Commerce administers the EAR (15 CFR §730-774), which regulate the export of "dual-use" items. These items include goods and related technology, including technical data and technical assistance, which are designed for commercial purposes, but which could have military applications, such as computers, aircraft, and pathogens.

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.

Facility Verification Request (FVR): The FVR is the official method of verifying the Facility Clearance Level and safeguarding capability of a NISP contractor. All Federal agencies and contractors participating in the National Industrial Security Program (NISP) are eligible to access the FVR. The FVR includes the Facility Name, CAGE Code, Physical Location Address, Classified Mailing Address, FCL Status/Level, and FCL Status/Level Date, Document Safeguarding Level, Special Limitations, FSO Name, FSO Phone, DSS Field Office, and assigned ISR Phone.

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 National: Any person who is not a citizen or national of the United States.

Foreign Visits System (FVS): The automated system operated by the Office of the USD(P) that provides staffing and database support for processing RFVs by foreign nationals to DoD Component activities and defense contractors.

Government Accountability Office (GAO): The audit, evaluation, and investigative arm of Congress.

Government Contracting Activity (GCA): 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 Security Oversight Office (ISOO): Office responsible for implementing and monitoring the NISP and for issuing implementing directives that shall be binding on agencies.

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.

International Traffic in Arms Regulations (ITAR): Sets forth the rules and procedures with respect to export of defense articles and defense services. This includes export of both classified and unclassified information.

International Visit Program (IVP): The DoD IVP is used to process visits and assignments of foreign nationals to the DoD Components and cleared contractor facilities. IVP is designed to ensure that classified information and CUI to be disclosed to visitors has been properly authorized for disclosure to their governments, to ensure that the requesting foreign government provides a Security Assurance for the proposed visitor when classified information is involved in the visit or assignment, and to facilitate administrative arrangements (e.g., date, time, and place) for the visit or assignment.

Joint Personnel Access System (JPAS): The DoD system of record for contractor eligibility and access for personnel security clearances. In the near future, JPAS will be replaced by the Defense Information System for Security (DISS).

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

Office of Personnel Management (OPM): The Office of Personnel Management (OPM) conducts a National Agency Check Plus Written Inquiries (NACI) and Access National Agency Check and Inquiries (ANACI) on Department of Defense (DoD) civilians and a broad range of Personnel Security Investigation (PSI) for other Federal agencies. Housed within OPM is the National Background Investigations Bureau (NBIB) established in 2016 as the primary service provider of government-wide background investigations for the Federal Government with the mission of delivering efficient and effective background investigations to ensure the integrity and trustworthiness of the Federal workforce.

National Industrial Security Program (NISP): The 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 (DoD 5220.22-M).

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

National Security Council (NSC): A governing entity responsible for providing overall policy direction for the NISP.

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.

North Atlantic Treaty Organization (NATO): NATO is an intergovernmental military alliance that consists of 29 independent member countries across North America and Europe. NATO constitutes a system of collective defense whereby its member states agree to mutual defense in response to an attack by any external party. Three NATO members (the United States, France and the United Kingdom) are permanent members of the United Nations Security Council with the power to veto and are officially nuclear-weapon states.

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.

Personnel Security Investigation (PSI): A non-criminal investigation that contains sufficient information for an adjudicator to make a determination that an individual is loyal, trustworthy, and reliable enough for access to classified information and/or assignment to a national security sensitive position. Also known as a national security background investigation.

Prime Contractor: The contractor who receives a prime contract from a GCA.

Request for Visit (RFV): Required for incoming international visits. The RFV may be submitted through the sponsoring government's embassy in Washington, D.C. or by the sponsoring organization using the automated Foreign Visits System (FVS) and IVP procedures. The cognizant U.S. Government agency approves or rejects the RFV.

SECRET: The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security that the original classification is able to identify or describe.

Security Assurance: The written confirmation requested by, and exchanged between governments, of the security clearance level or eligibility for clearance of their employees, contractors, and citizens. It includes a statement by a responsible official of a foreign government that the original recipient of U.S. classified information possesses the requisite security clearance, is approved by his or her government for access to information of the security classification involved on behalf of the foreign government, and that the recipient will comply with any security requirements specified by the U.S. In the case of contractors, security assurance includes a statement concerning the level of storage capability.

Sensitive Compartmented Information (SCI): SCI is derived from intelligence sources, methods, or analytical processes that is required to be handled within a formal control system established by the Director of Central Intelligence (DCI). SCI is a category of classification and control markings.

SF 312: Classified Information Nondisclosure Agreement

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 SERCRET, 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

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.

Technology Control Plan (TCP): The document that identifies and describes sensitive program information; the risks involved in foreign access to the information; the participation in the program or foreign sales of the resulting system; and the development of access controls and protective measures as necessary to protect the U.S. technological or operational advantage represented by the system.

TOP SECRET: The classification level applied to information, the unauthorized disclosure of which reasonable could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

Transmission: The sending of information from one place to another by audio, microwave, laser, or other non-connective methods, as well as by cable, wire, or other connective medium. Transmission also includes movement involving the actual transfer of custody and responsibility for a document or other classified material from one authorized addressee to another.

U-1201: The Request For Visit form used for international visits. This form and the instructions for its completion are located in Appendix B of the NISPOM.