Visits and Meetings in the NISP Glossary

Access: The actual level of classified information to which a person is authorized disclosure. It is a security officer's responsibility to assign access level.

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 Contractor Facility: Any industrial, educational, commercial facility, or other entity that has been granted a facility security clearance under the U.S. NISP.

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 E.O. 12829 to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to U.S. Industry. Department of Defense, the Department of Energy, the Central Intelligence Agency, and the Nuclear Regulatory Commission. When the DOD is the CSA, international visits are facilitated by DCSA Headquarters.

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 classified 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.

Counterintelligence (CI): Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, persons, their agents, or international terrorist organizations.

Critical Nuclear Weapon Design Information (CNWDI): A Department of Defense (DOD) category that reveals the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munition, or test device.

Defense Counterintelligence and Security Agency (DCSA): The security agency in the federal government dedicated to protecting America's trusted workforce and trusted workspaces — real or virtual. DCSA joins two essential missions: Personnel Vetting and Critical Technology Protection, supported by Counterintelligence and Training, Education and Certification functions.

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

Department of Defense (DOD): The largest of five CSAs, having issued the most classified contracts to industry. Additionally, the Secretary of Defense has entered into agreements with other federal agencies for the purpose of rendering industrial security services.

Department of Defense Consolidated Adjudications Facility (DOD CAF): The DOD CAF is the sole authority to determine security clearance eligibility of Non-Intelligence agency DOD personnel occupying sensitive positions and/or requiring access to classified material, including Sensitive Compartmented Information (SCI).

Department of Defense (DOD) Directive: A DOD Directive establishes policy, assigns responsibilities, and delegates authority to DOD Components.

Department of Defense (DOD) Directive 5230.20: This directive, "Visits and Assignment of Foreign Nationals", establishes policies and responsibilities governing visits and assignments of foreign nationals to DOD Components and cleared contractor facilities.

Department of Defense Form 254 (DD Form 254) – Contract Security Classification Specification: This document provides security guidance to both the contractor and the government. It is a legal document that directs the contractor about the proper protection of classified material released under the contract.

Department of Defense (DOD) Personnel Security System of Record: System of record for personnel security, suitability, and credential management of all DOD employees, military personnel, civilians, and contractors.

Eligibility: The highest level of information which may be disclosed to a person based on the type of completed and favorable investigation. It is a CAF responsibility to assign eligibility.

Empowered Official: The ITAR defines an Empowered Official as a U.S. person: Employed by the applicant/subsidiary with authority for policy or management; Legally empowered to sign license applications or requests on behalf of the applicant; Understands the requirements of export control statutes and penalties for violating the AECA and ITAR; and Authorized to: Enquire into a proposed export, temporary import, or brokering activity; and Verify legality and accuracy; and Refuse to sign any license application or other request.

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.

Export authorization: An approved numbered license or agreement or an authorized exemption under the ITAR. Written approval by a GCA of a visit request is considered to be the export authorization if the approval clearly identifies the information that will be disclosed.

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 national security standpoint, a facility is eligible for access to classified information at the same or lower classification category as the clearance being granted. The FCL may be granted at the Confidential, Secret, or Top Secret level.

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.

FCL System of Record: The electronic system that all companies must use while in process for an FCL or to report a changed condition. It is also a repository of information about DOD cleared contractor facilities. The system has internal users (with full access such as DCSA personnel) and external users (with limited access).

Foreign interest: Any foreign 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: In accordance with the NISPOM, any person who is not a citizen or national of the United States.

Foreign person: Foreign person means any natural person who is not a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any foreign corporation, business association, partnership, trust, society or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions).

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-approved arrangement: A Government-approved arrangement may be an agreement, contract, or export license.

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

International Traffic in Arms Regulations (ITAR): Control the export and import of defense-related articles and services on the U.S. Munitions List (defense and military-related technologies).

International Visit Program (IVP): International Visits Program (IVP): Is designed to ensure that classified information and CUI to be disclosed to such 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.

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.

National Industrial Security Program Operating Manual (NISPOM) – 32CFR Part 117: Implements policy, assigns responsibilities, establishes requirements, and provides procedures consistent with Executive Order 12829, "National Industrial Security Program;" Executive Order 10865, "Safeguarding Classified Information within Industry;" and 32 Code of Regulation Part 2004, "National Industrial Security Program." That guidance outlines the protection of classified information that is disclosed to, or developed by contractors, licensees, grantees, or certificate holders to prevent unauthorized disclosure.

Need-to-Know: 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.

North Atlantic Treaty Organization (NATO) Facility Security Clearance Certificate (FSCC): This certificate is required for any contractor to negotiate or perform on a NATO classified contract or subcontract. The certificate certifies the facility has a U.S. facility security clearance at the requisite level, its personnel who require access have been briefed on NATO procedures, and the requirements of the NISPOM are met. The DOD Cognizant Security Agency will provide the certificate to the requesting NATO command, agency or member nation, as applicable.

Personally Identifiable Information (PII): 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): The 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 Security Clearance being granted.

Portable Electronic Device (PED): Mobile devices that transmit, store, or record data. Examples range from handheld, lightweight electronic devices such as tablets, e-readers, and smartphones to small devices, such as MP3 players.

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 regarding 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.

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.

United States (U.S.): The 50 states and the District of Columbia.

Visit Authorization Letter (VAL): This letter may be used if the DOD Personnel Security System of Record is not available. The letter must state the requesting contractor's name, address, phone number, CAGE Code, if applicable, and certification of the level of the favorable entity eligibility determination (also referred to as a Facility Clearance, or FCL and the date or period during which the VAL is to be valid.