Glossary

Course: Developing a Security Education and Training Program

AIS: Automated Information System

Awareness: A security education program should include components designed to increase security awareness, or everyday consciousness on the part of personnel, of security threats and vulnerabilities.

CI: Counterintelligence

Classified Information Nondisclosure Agreement: SF 312

Classified Information Procedures Act: A law that provides a mechanism for the courts to determine what classified information defense counsel may access.

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

Classifier: Any person who makes a classification determination and applies a classification category to information or material. The determination may be an original classification action or it may be a derivative classification action. Contractors make derivative classification determinations based on classified source material, a security classification guide, or a Contract Security Classification Specification.

CNWDI: Critical Nuclear Weapons Design Information, CNWDI, is TOP SECRET RESTRICTED DATA or SECRET RESTRICTED DATA that reveals the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition, munitions, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high-explosive materials by type.

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.

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.

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.

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

Courier: A designated, cleared employee, whose principal duty is to transmit classified material to its destination. The classified material remains in the personal possession of the courier except for authorized overnight storage.

CRYPTO: CRYPTO is a marking or designator identifying COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. Government or U.S. Government-derived information (per CNSSI No 4009, National IA Glossary).

DD Form 254: Contract Security Classification Specification

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

Declassification: The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with removal or cancellation of the classification designation.

Defense Security Service (DSS): The Defense Security Service (DSS) is an agency of the Department of Defense (DoD) located in Alexandria, 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, 23 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 Academy: A function within the Defense Security Service that provides security education and training to DoD and other U.S. Government personnel and contractors.

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 Defense Industrial Security Clearance Office (DISCO): Office within the Defense Security Service that processes requests for, and other actions related to personnel security clearances for personnel from facilities participating in the NISP.

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

Defense Security Service, Information Systems Security Professional: 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.

Derivative Classification: The incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification. Persons who apply derivative classification markings shall observe and respect original classification decisions and carry forward to any newly created documents any assigned authorized markings.

Document: Any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

Downgrade: A determination that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect a lower degree of protection.

Education: The purpose of security education is to communicate the underlying principles and rationales of a security program so that personnel understand the importance of their role in providing security.

Eligibility: A central Adjudication facility (CAF) has made an adjudicative determination of member Personnel Security investigation (PSI) and that member may have access to classified information equal to level of investigation adjudicated.

Escort: A designated, cleared person, who accompanies a shipment of classified material to its destination. The classified material does not remain in the personal possession of the escort but the conveyance in which the material is transported remains under the constant observation and control of the escort.

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 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.

Foreign Government Information (FGI): Information that is: a. Provided to the U.S. by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or b. Produced by the U.S. pursuant to, or as a result of, a joint arrangement with a foreign government or governments, an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence.

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

Generational differences: With a multigenerational work force, you will have an audience with a range of experiences, expectations, and comfort levels with technology. Keep in mind the distinct needs of Baby Boomers, Gen-Xers, and Millenials when designing your training. There is a great deal of interesting research on generational differences and their effect on how people approach work and learning.

Handcarrier: A designated, cleared employee, who occasionally hand carries classified material to its destination in connection with a classified visit or meeting. The classified material remains in the personal possession of the handcarrier except for authorized overnight storage.

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

Industrial Security Representative (ISR or IS Rep): The person who represents the Defense Security Service for security matters that are covered by the NISP.

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.

Information Management System (IMS): A system to protect and control classified information as required by NISPOM paragraph 5-200. The IMS employed by a contractor must be capable of facilitating retrieval and disposition of classified material in a reasonable period of time.

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 (IS): 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): 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.

Information System Security Professional (ISSP): An employee of Defense Security Service assigned to the ODAA or to a DSS field element who provides advice and assistance and participates in certification and inspections of information systems. An ISSP is a subject matter expert on information systems security in the NISP.

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 operations.

Job responsibilities: Personnel with different job responsibilities will have different needs and expectations for their training. Consider how analysts vs. administrative support staff vs. technological staff might have different content needs and comfort levels with technology. You should work to ensure that the content of the training is relevant to the audience, that is, that it covers the security responsibilities of the particular people who receive the training.

Joint Personnel Access System (JPAS): The DoD system of record for contractor eligibility and access for personnel security clearances.

JCAVS: JPAS is comprised of two major subsystems, the Joint Adjudication Management System (JAMS) and the Joint Clearance and Access Verification System (JCAVS). JPAS = JAMS + JCAVS

> JAMS provides Central Adjudication Facilities (CAFs) a single information system to assist in the adjudication process and standardizes core DoD Adjudication processes. JAMS is used by adjudicators to record eligibility determinations and command access decisions, and promotes reciprocity between the DoD CAFs.
>
> JCAVS is one of the two major subsystems of JPAS JCAVS provides security personnel the ability to constantly view eligibility information and update access information in real time. JCAVS also provides users the ability to constantly communicate with other Security Management Offices and CAFs.

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.

Learning styles: Traditional classroom training tends to rely heavily on lecture, but not all learners find listening the most effective way to learn. Some people are highly visual and learn best from pictures, graphs, and other visual aids. Others need to actually

perform a task to learn how to do it. When analyzing your audience, determine whether they prefer learning visually, by listening, or by doing. Then, when you design your training, be sure to include elements for all types of learners.

Limited Access Authorization (LAA): Security access authorization to CONFIDENTIAL or SECRET information granted to non-U.S. citizens requiring such limited access in the course of their regular duties.

Material: Any product or substance on or in which information is embodied.

Motivation: Motivation is critical to a security education program because it is the element that gives individuals a personal stake in the outcome, increasing the odds that they will proactively contribute to the program.

NATO Information: Information bearing NATO markings, indicating the information is the property of NATO, access to which is limited to representatives of NATO and its member nations unless NATO authority has been obtained to release outside of NATO.

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.

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.

Network: A system of two or more IS that can exchange data or information.

Original Classification: An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required. (Only government officials who have been designated in writing may apply an original classification to information.)

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.

Proscribed Information: a. Top Secret information; b. COMSEC information, except classified keys used for data transfer; c. RD as defined in reference (c); d. SAP information; or e. SCI.

Restricted Area: A controlled access area established to safeguard classified material, that because of its size or nature, cannot be adequately protected during working hours by the usual safeguards, but that is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the CSA.

Restricted Data (RD): All data concerning the design, manufacture, or use of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the RD category pursuant to section 142 of reference (c).

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

Security-in-Depth: A determination made by the CSA that a contractor's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility.

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

SF 312: Classified Information Nondisclosure Agreement

Source Document: A classified document, other than a classification guide, from which information is extracted for inclusion in another document.

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 reference (b).

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.

Training: The purpose of security training is to inform personnel of their security responsibilities and allow them to gain the skills and knowledge they need to successfully protect national security.

Transmission: The sending of information from one place to another by radio, 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.

Unauthorized Person: A person not authorized to have access to specific classified information in accordance with the requirements of this Manual.

United States: The 50 states and the District of Columbia.

United States and its Territorial Areas: The 50 states, the District of Columbia, Puerto Rico, Guam, American Samoa, the Virgin Islands, Wake Island, Johnston Atoll, Kingman Reef, Palmyra Atoll, Baker Island, Island, and Northern Mariana Islands. *NOTE: From 18 July 1947 until 1 October 1994, the United States administered the Trust Territory of the Pacific Islands; it entered into a political relationship with all four political units: the Northern Mariana Islands is a commonwealth in political union with the United States (effective 3 November 1986); the Republic of the Marshall Islands signed a Compact of Free Association with United States (effective 21 October 1986); the Federated States of Micronesia signed a Compact of Free Association with the United States (effective 3 November 1986); Palau concluded a Compact of Free Association with the United States (effective 1 October 1994).*

U.S. Person: Any form of business enterprise or entity organized, chartered, or incorporated under the laws of the United States or its territories and any person who is a citizen or national of the United States.

Upgrade: A determination that certain classified information, in the interest of national security, requires a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a higher degree.

Working Hours: The period of time when: a) there is present in the specific area where classified material is located, a work force on a regularly scheduled shift, as contrasted with employees working within an area on an overtime basis outside of the scheduled work shift; and b) the number of employees in the scheduled work force is sufficient in number and so positioned to be able to detect and challenge the presence of unauthorized personnel. This would, therefore, exclude janitors, maintenance personnel, and other individuals whose duties require movement throughout the facility.