Glossary

NISP Security Violations and Administrative Inquiries

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

Adjudication: Evaluation of personnel security investigations and other relevant information to determine if it is clearly consistent with the interests of national security for persons to be granted or retain eligibility for access to classified information, and continue to hold positions requiring a trustworthiness decision

Administrative Inquiry: Formal investigation of a possible loss, compromise or suspected compromise

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

Authority: The reason for an inquiry, when and where it was conducted, and who conducted the inquiry

Carelessness: Failure to give sufficient attention to avoiding harm or errors; negligence

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

Classification Review: Review of compromised classified information to determine whether affected information should be declassified or downgraded and identify measures to protect against threat to national security

Clearance: An administrative authorization for access to National Security Information (NSI) up to a stated classification level (TOP SECRET, SECRET, CONFIDENTIAL)

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

Cognizant Security Agencies (CSAs): Agencies of the Executive Branch that have been authorized by Executive Order 12829 to establish an industrial security

program to safeguard classified information under the jurisdiction of these agencies when disclosed or released to U.S. Industry. These agencies are The Department of Defense, Office of the Director of National Intelligence, Department of Energy, Nuclear Regulatory Commission, and Department of Homeland Security.

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

Compromise: An unauthorized disclosure of information. A compromise is a confirmed disclosure of specifically identifiable classified information to specified unauthorized individuals(s).

Conclusion: A formal determination for each security violation as previously identified (loss, compromise, suspected compromise). Define the security violation as a Loss, Compromise, Suspected Compromise, or No Loss, Compromise, or Suspected Compromise. Include vulnerability of information, description of unauthorized access, and description of GCA classification review.

CONFIDENTIAL: The classification level applied to information, the unauthorized disclosure of which could reasonably be expected to cause damage to National Security that the Original Classification Authority (OCA) is able to identify or describe

Containment: Keeping security violations from harming other programs or individuals

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

Corrective Actions: Any disciplinary actions taken against a culpable individual(s) involved in a security violation and the actions initiated or taken by the facility to secure the information after the violation

Culpable Person: An individual involved in a security violation that has been determined to have displayed a deliberate disregard for security requirements, had a pattern of negligence, or was grossly negligent in their duties

Damage Assessment: The analysis of the impact on national security because of the disclosure of classified information to an unauthorized person

Data Spill: Known also as contaminations or classified message incidents, occurs when classified data or controlled unclassified data (CUI) is introduced to an unclassified computer system or to a computer system accredited at a lower classification level than the data being entered

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

DSS supports the National Security and the warfighter, secures the nation's technological base, and oversees the protection of U. S. and foreign classified information in the hands of industry. DSS 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, Center for Development of Security Excellence (CDSE): Responsible for providing security education and training to DoD and other U.S. government personnel, DoD contractors, and sponsored representatives of foreign governments

Defense Security Service, 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, Field Counterintelligence Specialist (FCIS): Assists FSOs in identifying potential threats to U.S. technology and developing CI awareness and reporting by company employees

Defense Security Service, Field Office Chief (FOC): Manages the field offices that are staffed by Industrial Security Representatives (IS Reps). The Field Office Chief is responsible for ensuring that each facility is assigned an IS Rep.

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

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

process of getting your information systems accredited to process classified information

Defense Security Service, Office of Designated Approving Authority (ODAA): Office within the Defense Security Service that facilitates the certification and accreditations process for information systems at cleared contractor facilities

Defense Security Service, Personnel Security Management Office for Industry (PSMO-I): 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, Regional Director: A DSS employee that has overarching responsibility of one of the four DSS geographical regions: Capital, Northern, Southern, and Western

Department of Defense: The largest Cognizant Security Agency (CSA) with the most classified contracts with industry

Department of Defense Consolidated Adjudication Facility: Responsible for issuing a clearance authorization for eligible individuals

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

Downgrading: A determination by a Declassification Authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level

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.

Essential Facts: Provide description of the circumstances surrounding the violation, the relevant sections of the NISPOM that were violated, who was involved, and when and where the violation occurred. Include the level and type of personnel clearance of the individuals involved in the occurrence.

Espionage: The act or practice of spying or of using spies to obtain secret intelligence. Overt, covert, or clandestine activity, usually used in conjunction with the country against which such an activity takes place (e.g., espionage against the United States (U.S.)).

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 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

Federal Bureau of Investigations (FBI): An intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities—the principal investigative arm of the U.S. Department of Justice and a full member of the U.S. Intelligence Community

Foreign Involvement: The fact or condition of being involved with a foreign country

Freedom of Information Act (FOIA): A provision that any person has a right, enforceable in court, of access to federal agency records, except to the extent that such records, or portions thereof, are protected from disclosure by one of nine exemptions

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

Inadvertent Exposure: A set of circumstances or a security incident in which a person has had involuntary access to classified information that he or she was or is not normally authorized

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

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

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

Information System: 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.

Investigation: The action of investigating something or someone; formal or systematic examination or research

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

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. Facility Security Officers (FSOs) are considered KMP.

Loss: Classified information that is or was outside the custodian’s control and the classified information cannot be located or its disposition cannot be determined

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

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

National Security Agency (NSA): Provides information assurance services and information and signals intelligence

Negligence: Failure to use reasonable care, resulting in damage, loss or injury to another

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

Preliminary Inquiry: Done to secure the classified information and gather all the facts to determine if there was a loss, compromise, or suspected compromise

Sabotage: The willful destruction of government property with the intent to cause injury, destruction, defective production of national defense, or war materials by either an act of commission or omission

Safeguarding: Controls that are prescribed to protect classified information

SECRET: The classification level applied to information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to National Security that the Original Classification Authority (OCA) is able to identify or describe

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 Assessment: Reviews of contractor security programs to ensure security counter measures are in place to mitigate hostile intelligence threats and ensure national policy compliance

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.

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

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

Subversion: An attempt to transform the established social order and its structures of power, authority, and hierarchy

Suspected Compromise: Occurs whenever identifiable classified information has been made available to unauthorized individual(s) who may have gained access to the information

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

Technology: The information and know-how (whether in tangible form, such as models, prototypes, drawings, sketches, diagrams, blueprints, or manuals, or in intangible form, such as training or technical services) that can be used to design, produce, manufacture, utilize, or reconstruct goods, including computer software and technical data, but not the goods themselves, or the technical information and know-how that can be used to design, produce, manufacture, use, or reconstruct goods, including technical data and computer software

Terrorism: The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological

Threat: Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or Denial of Service (DOS)

TOP SECRET: The classification level applied to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to National Security that the Original Classification Authority (OCA) is able to identify or describe

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