Counterintelligence Glossary

A==========

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

Acquisition Special Access Program (ASAP): A Special Access Program (SAP) established primarily to protect sensitive research, development, testing, and evaluation or procurement activities in support of sensitive military and intelligence requirements.

Acquisition Systems Protection (ASP): The safeguarding of defense systems anywhere in the acquisition process as defined in Department of Defense (DOD) Directive 5000.1; defense technologies being developed that could lead to weapon or defense systems and defense research data.

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.

Adjudication Facility: A facility with assigned adjudicators certified to evaluate Personnel Security Investigations (PSI) and other relevant information to determine if granting or continuing national security eligibility is clearly consistent with the interests of national security. The DOD consolidated adjudications facility is known as the DOD Central Adjudication Facility (CAF).

Alternative Compensatory Control Measures (ACCM): Measures designed to safeguard sensitive intelligence and operations when normal security measures are either not sufficient to achieve strict controls over access to information or where strict SAP access controls are either not required or are too stringent.

Analysis: The process by which information is transformed into intelligence; a systemic examination of information to identify significant facts, make judgments, and draw conclusions.

Anomalous Health Incident (AHI): Unexplained sensory events coupled with physical symptoms, including some combination of sounds or sensations of sounds, pressure, vibrations, heat, and/or unexplained physical discomfort such as pain, nausea, and disequilibrium.

Anomaly: Activity or knowledge, outside the norm, that suggests a foreign entity has foreknowledge of U.S. information, processes, or capabilities.

Antiterrorism (AT): Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces.

Arms Export Control Act (AECA): The basic U.S. law providing the authority and general rules for the conduct of foreign military sales and commercial sales of defense articles, defense services, and training. The AECA came into existence with the passage of the Foreign Military Sales Act (FMSA) of

1968. An amendment in the International Security Assistance and Arms Export Control Act of 1976 changed the name of FMSA to the AECA.

Assets: A person, structure, facility, information, material, or process that has value.

Attempted Acquisition of Technology (AAT): A method of operation. Acquiring protected information in the form of controlled technologies, via direct contact or through the use of front companies or intermediaries, including the equipment itself or diagrams, schematics, plans, spec sheets, or the like.

C==========

Caveat: A designator used with or without a security classification to further limit the dissemination of restricted information.

Central Intelligence Agency (CIA): An independent U.S. Government agency responsible for providing national security intelligence to senior U.S. policymakers. The CIA's primary mission is to collect, analyze, evaluate, and disseminate foreign intelligence to assist the President and senior U.S. government policymakers.

Classification: The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

Classified Contract: Any contract, license, agreement, or grant requiring access to classified information by a contractor and its employees for performance. A contract is referred to in this rule as a "classified contract" even when the contract document and the contract provisions are not classified. The requirements prescribed for a "classified contract" also are applicable to all phases of precontract, license or grant activity, including solicitations (bids, quotations, and proposals), precontract negotiations, post-contract activity, or other government contracting activity (GCA) programs or projects which require access to classified information by a contractor.

Classified Information: Information that has been determined pursuant to Executive Order (EO) 13526, or any successor order, EO 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011) to require protection against unauthorized disclosure and that is marked to indicate its classified status when in documentary form.

Classified Information Spillage: A security incident that occurs whenever classified data is spilled either onto an unclassified information system or to an information system with a lower level of classification or different security category.

Clearance: A formal security determination by an authorized adjudicative office that an individual has authorized access, on a need to know basis, to a specific level of collateral classified information (TOP SECRET, SECRET, CONFIDENTIAL).

Cleared Contractor (CC): A person or facility operating under the National Industrial Security Program (NISP) that has had an administrative determination that they are eligible, from a security point of view, for access to classified information of a certain level (and all lower levels).

Cleared Contractor Facility: Any industrial, educational, commercial facility, or other entity that has been granted a facility security clearance under the U.S. National Industrial Security Program (NISP).

Cleared Defense Contractor (CDC): A subset of contractors cleared under the National Industrial Security Program (NISP): who have contracts with the Department of Defense (DOD). Therefore, not all cleared contractors have contracts with DOD.

Cleared Employee: A person who has been granted access to classified information, other than the President and Vice President, employed by, or detailed or assigned to, a department or agency, including members of the Armed Forces; an expert or consultant to a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.

Communications Security (COMSEC): The protection resulting from all measures designed to deny unauthorized persons' information of value that might be derived from the possession and study of telecommunications or to mislead unauthorized persons in their interpretation of the results of such possession and study.

Compromise: An unauthorized disclosure of classified information.

Conferences, Conventions, and Tradeshows: A method of contact. Contact regarding or initiated during an event, such as a conference, convention, exhibitions, or tradeshow.

Confidential: Information or material of which unauthorized disclosure could reasonably be expected to cause damage to the national security that the Original Classification Authority (OCA) is able to identify or describe.

Contact: Any form of meeting, association, or communication in person by radio, telephone, letter, computer, or other means, regardless of who initiated the contact for social, official, private, or other reasons.

Continuous Vetting (CV): CV involves regularly reviewing a cleared individual's background to ensure they continue to meet security clearance requirements and should continue to hold positions of trust. Automated record checks pull data from criminal, terrorism, and financial databases, as well as public records, at any time during an individual's period of eligibility. When the Defense Counterintelligence and Security Agency (DCSA) receives an alert, it assesses whether the alert is valid and worthy of further investigation. DCSA investigators and adjudicators then gather facts and make clearance determinations. CV helps DCSA mitigate personnel security situations before they become larger

problems, either by working with the cleared individual to mitigate potential issues, or in some cases suspending or revoking clearances.

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.

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, or persons or their agents, or international terrorist organizations or activities.

Counterintelligence Investigation: Formal investigative activities undertaken to determine whether a particular person is acting for or on behalf of, or an event is related to, a foreign power engaged in spying or committing espionage, sabotage, treason, sedition, subversion, assassinations, or international terrorist activities, and to determine actions required to neutralize such acts.

Counterintelligence Special Agent (CISA): Credentialed counterintelligence (CI) agents from the Defense Counterintelligence and Security Agency (DCSA) serving the cleared industry and academia community.

Countermeasure: The employment of devices or techniques that impair the operational effectiveness of enemy activity. Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities.

Critical Program Information (CPI): U.S. capability elements that contribute to the warfighters technical advantage, which if compromised, undermines U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment.

Critical Technology: Technology or technologies essential to the design, development, production, operation, application, or maintenance of an article or service that makes or could make a significant contribution to the military potential of any country, including the U.S.

Cyber Operations: A method of contact. Activities taken directly against a targeted system; to include cyber network attack, cyber network exploitation, and collection.

D==========

Damage Assessment: A determination of the effect of a compromise of classified information on national security.

Declassification: A date or event which coincides with the lapse of the information's national security sensitivity, as determined by the original classification authority (OCA). Declassification occurs when the OCA has determined that the classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, and the information has had its classification designation removed or cancelled.

Defense Advanced Research Projects Agency (DARPA): A Defense Agency that serves as the research and development (R&D) organization in DOD with a primary responsibility of maintaining U.S. technological superiority over our adversaries.

Defense Counterintelligence and Security Agency (DCSA): DCSA is 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 Industrial Base (DIB): The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development and design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements.

Defense Information Security System (DISS): DISS serves as the enterprise-wide solution for personnel security, suitability, and credentialing management for DOD military, civilian, and contractors. DISS replaced the Joint Personnel Adjudication System (JPAS) as the System of Record on March 31, 2021. An innovative, web-based application, the platform provides secure communications between adjudicators, security officers, and components, allowing users to request, record, document, and identify personnel security actions. DISS will be an integral step toward the National Background Investigation Services (NBIS) platform currently in development and full implementation of the government-wide policy to overhaul the personnel vetting process known as Trusted Workforce 2.0

Defense Intelligence Agency (DIA): A DOD agency and a member of the U.S. Intelligence Community responsible for providing timely, objective, and cogent military intelligence to warfighters, defense planners, and defense and national security policymakers.

Defense Personnel Security Research Center (PERSEREC): A DOD entity dedicated to improving the effectiveness, efficiency, and fairness of the DOD personnel security system.

Deliberate Compromise: The act, attempt, or contemplation of intentionally conveying classified documents, information, or material to any unauthorized person, including public disclosure, or the intentional misuse or mishandling of classified information.

Department of Homeland Security (DHS): A cabinet department of the U.S. federal government. DHS has five missions: (1) Prevent terrorism and enhance security; (2) Secure and manage U.S. borders; (3) Enforce and administer immigration laws; (4) Safeguard and secure cyberspace; and (5) Ensure resilience to disasters.

Disinformation: Disinformation is deliberately created content to mislead, harm, or manipulate a person, social group, organization, or country.

Dual-use: Technology and articles that are potentially used either for commercial/civilian purposes or for military, defense, or defense-related purposes.

Due Diligence: The technical term for the necessary assessment of the past performance, reputation, and future plans of a prospective alliance partner, private sector, or other entity, with regard to various business practices and principles. This assessment of a prospective alliance partner would normally involve, at a minimum, examining their social, environmental, and financial track records. In terms of Supply Chain Risk Management (SCRM), due diligence refers to assessing first-tier suppliers regularly to increase visibility into third-party suppliers and service providers; and leveraging this data to properly vet vendors providing key components to critical systems and networks.

E==========

Economic Espionage: The knowing misappropriation of trade secrets with the knowledge or intent that the offense will benefit a foreign government, foreign instrumentality, or foreign agent. Misappropriation includes, but is not limited to, stealing, copying, altering, destroying, transmitting, sending, receiving, buying, possessing, or conspiring to obtain trade secrets without authorization.

Economic Espionage Act (EEA): The Economic Espionage Act of 1996 criminalizes two forms of trade secret theft: 1) theft for the benefit of a foreign entity (economic espionage – 18 U.S. Code §1831) and 2) theft for pecuniary gain (theft of trade secrets – 18 U.S. Code §1832), commonly referred to as industrial espionage.

Elicitation: In intelligence usage, the acquisition of information from a person or group in a manner that does not disclose the intent of the interview or conversation.

Eligibility: A national security eligibility is a determination that a person is able and willing to safeguard classified national security information and/or occupy a national security sensitive position.

Email: Electronic mail. As a method of contact, this refers to unsolicited requests received via email for information or purchase requests.

Employee: For purposes of the National Insider Threat Policy, "employee" has the meaning provided in section 1.1(e) of Executive Order (EO) 12968; specifically: a person, other than the President and Vice President, employed by, detailed or assigned to, a department or agency, including members of the Armed Forces; an expert or consultant to a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.

Espionage: Espionage is a national security crime; specifically, it violates Title 18 USC, §§ 792-798 and Article 106a, Uniform Code of Military Justice (UCMJ). Espionage convictions require the transmittal of national defense information with intent to aid a foreign power or harm the U.S. However, even gathering, collecting, or losing national defense information can be prosecuted under Title 18.

Espionage Indicators: Warning signs that an insider may be working for or is susceptible to control by a Foreign Intelligence Entity (FIE). These warning signs are the result of an insider's actions, activities, and behaviors that may be indicative of potential espionage-related activity.

Essential Elements of Friendly Information (EEFI): Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness.

Executive Order 12333: Authorizes elements of the Intelligence Community to collect, retain, or disseminate information concerning U.S. persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General.

Exploitation of Business Activities: A method of operation. Establishing a commercial relationship via joint ventures, partnerships, mergers and acquisitions, foreign military sales, or service provider; leveraging an existing commercial relationship in order to obtain access to personnel or protected information and technology.

Exploitation of Cyber Operations: A method of operation. Foreign intelligence entities or other adversaries compromising the confidentiality, integrity, or availability of targeted networks, applications, credentials or data with the intent to gain access to, manipulate, or exfiltrate personnel information or protected information and technology.

Exploitation of Experts: Gaining a method of operation. access to personnel or protected information and technology via requests for, or arrangement of, peer or scientific board review of academic papers or presentations; requesting a consult with faculty members or subject matter experts; or attempting to invite or otherwise entice subject matter experts to travel abroad or consult for foreign entities.

Exploitation of Insider Access: A method of operation. Trusted insiders exploiting their authorized placement and access within cleared industry or cause other harm to compromise personnel or protected information and technology.

Exploitation of Relationships: A method of operation. Leveraging existing personal or authorized relationships to gain access to protected information.

Exploitation of Security Protocols: A method of operation. Visitors or unauthorized individuals circumventing or disregarding security procedures or behaviors by cleared or otherwise authorized persons that indicate a risk to personnel or protected information and technology.

Exploitation of Supply Chain: A method of operation. Compromising the supply chain, which may include the introduction of counterfeit or malicious products or materials into the supply chain with the intent to gain unauthorized access to protected data, alter data, disrupt operations, or interrupt communication.

Export Administration Regulations (EAR): EAR-controlled items are those that can be used both in military and other strategic uses and in commercial applications.

F==========

Facility Security Officer (FSO): The security officer for a cleared defense contractor facility; the FSO supervises and directs security measures necessary for implementing requirements for classified information.

Federal Bureau of Investigation (FBI): The FBI has primary responsibility for Counterintelligence (CI) investigations within the U.S. DOD.

FIVE EYES (FVEY): An intelligence alliance comprising the U.S., Australia, Canada, New Zealand, and the United Kingdom.

Foreign Intelligence Entity (FIE): Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. This term includes a foreign intelligence and security service and international terrorist organizations.

Foreign Intelligence Threat: The all-source intelligence threat posed by foreign intelligence entities to U.S. interests.

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 U.S. or its territories, and any person who is not a citizen or national of the U.S.

Foreign Military Sales (FMS): That portion of U.S. security assistance for sales programs that require agreements/contracts between the U.S. Government and an authorized recipient government or international organization for defense articles and services to be provided to the recipient for current stocks or new procurements under DOD-managed contracts, regardless of the source of financing.

Foreign Ownership, Control or Influence (FOCI): A U.S. company is considered under foreign ownership, control, or influence whenever a foreign interest has the power, direct or indirect, whether or not exercised and whether or not exercisable through ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner that may result in unauthorized access to classified information or may affect adversely the performance of classified matters.

Foreign Visit: A foreign national enters or proposes to enter a DOD Component or cleared contractor facility or to meet with employees or representatives of the facility. As a method of contact, activities or contact occurring before, during, or after a visit to a contractor's facility.

Front Company: A company or business entity that is established, used, or co-opted for an illicit purpose; wherein the management, control, influence, or criminal activities are being directed by a hidden or disguised individual or group.

G==========

Government-Owned Contractor Operated (GOCO): A manufacturing plant that is owned by the government and operated by a civilian organization under contract to the government.

H==========

Hacker: Unauthorized user who attempts to or gains access to an information system.

Human Intelligence (HUMINT): Human Intelligence uses people to gather information.

I==========

Imagery Intelligence (IMINT): Imagery Intelligence uses satellite imagery, photographs, and other images to collect information.

Industrial Base Technology List (IBTL): The Defense Counterintelligence and Security Agency (DCSA)-developed list is a compendium of the science and technology capabilities under development worldwide that have the potential to significantly enhance or degrade U.S. military capabilities in the future. IBTL categories are correlated with legacy Military Critical Technology List (MCTL) categories.

Industrial Espionage: The knowing misappropriation of trade secrets related to, or included in, a product that is made for or placed in interstate or foreign commerce to the economic benefit of anyone other than the owner, with the knowledge or intent that the offense will injure the owner of that trade secret.

Information Security: The security discipline concerned with implementation of a system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure information that is authorized protection by Executive Order (EO), statute, or regulation. Information security includes protection of classified, controlled unclassified, and sensitive compartmented information.

Insider: Any person with authorized access to any U.S. Government resource, to include personnel, facilities, information, equipment, networks, or systems.

Insider Threat (InT): The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the U.S. This threat can include damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

Intelligence Community Directive (ICD) 700: Establishes Intelligence Community policy for the protection of national intelligence and provides framework for greater coordination and communications between CI and security activities of the Intelligence Community to strengthen the ability to identify, deter, disrupt, mitigate, and counteract intelligence activities directed against U.S. interests by foreign powers or activities.

Intelligence Community Directive (ICD) 750: Establishes the baseline for counterintelligence (CI) programs across the Intelligence Community to create a strategic approach to CI that will enhance the national security posture of the U.S. The ICD 750 recommends CI to be functionally integrated with security programs per the ICD 700.

Intelligence Oversight: The process of independently ensuring all DOD intelligence, counterintelligence (CI), and intelligence-related activities are conducted in accordance with applicable U.S. law, Executive Orders (EOs), Presidential directives, and DOD issuances designed to balance the requirement for acquisition of essential information by the Intelligence Community (IC), and the protection of Constitutional and statutory rights of U.S. persons.

Intelligence Report (INTREP): A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information.

Intelligence Threat: The intention, opportunity, and capability of any adversary to acquire and exploit critical information. The purpose of the acquisition is to gain a competitive edge or diminish the success of a particular U.S program, operations, or industrial activity.

International Traffic in Arms Regulations (ITAR): The International Traffic in Arms Regulations (ITAR) implements the provisions of the Arms Export Control Act (AECA) and controls the export and import of defense-related articles and services on the U.S. Munitions List.

Internet of Things (IoT): Networks of objects that communicate with other objects and with computers through the Internet. "Things" may include virtually any object for which remote communication, data collection, or control might be useful, such as vehicles, appliances, medical devices, electric grids, transportation infrastructure, manufacturing equipment, or building systems.

Investigation: The systematic inquiry into an allegation of unfamiliar or questionable activities wherein evidence is gathered to substantiate or refute the allegation or questionable activity. An investigation is initiated when there are articulable facts that indicate a possible violation of law or policy.

J==========

Joint Venture: An association of two or more persons or entities engaged in a single defined project with all parties contributing assets and efforts and sharing in the management, profits, and losses, in accordance with the terms of an agreement among the parties.

K==========

Key Facilities List: A register of selected command installations and industrial facilities of primary importance to the support of military operations or military production programs. It is prepared under the policy direction of the Joint Chiefs of Staff.

Key Management Personnel (KMP): KMP are an entity's senior management official (SMO), facility security officer (FSO), insider threat program senior official (ITPSO), and all other entity officials who either hold majority interest or stock in or have direct or indirect authority to influence or decide issues affecting the management or operations of, the entity or classified contract performance.

L==========

Life Cycle (Weapon System): All phases of the system's life including Research, Development, Test, and Evaluation (RDT&E); production; deployment; Operations and Support (O&S); and disposal.

M==========

Mail: As a method of contact, contact initiated via mail or post.

Malinformation: Malinformation is based on fact, but used out of context to mislead, harm, or manipulate.

Measures and Signatures Intelligence (MASINT): MASINT is technically derived intelligence that uses the unique characteristics of fixed and dynamic target sources.

Methods of Contact: Approaches used to connect the foreign actor to the targeted individual, information, network, or technology in order for the foreign actor to execute the Methods of Operation (MO).

Methods of Operation: Distinct patterns or methods of procedure thought to be characteristic of or habitually followed by an individual or organization involved in intelligence activity. These generally include the attempted acquisition of technology; exploitation of business activities; exploitation of cyber operations; exploitation of experts; exploitation of insider access; exploitation of relationships; exploitation of security protocols; exploitation of supply chain; résumé submission; request for information/solicitation; search/seizure; surveillance; and theft.

Military Department Counterintelligence Organization (MDCO): Elements of the military departments authorized to conduct counterintelligence (CI) investigations, i.e., Army CI, Naval Criminal Investigative Service, and the Air Force Office of Special Investigations.

Misinformation: Misinformation is false, but not created or shared with the intention of causing harm.

Modus Operandi (MO): A distinct pattern or method of procedure thought to be characteristic of or habitually followed by an individual or an organization involved in criminal or intelligence activity.

Motivation: The complex of reasoning and emotional or other drives that induces a person to accept employment or cooperate with an agency for a particular assignment.

N==========

National Access Elsewhere Security Oversight Center (NAESOC): NAESOC is designed to provide consistent oversight and security management for select facilities who do not possess classified information on-site ("access elsewhere").

National Background Investigation Services (NBIS): NBIS is the platform currently in development to replace Defense Information Security System (DISS) as the enterprise-wide solution for personnel security, suitability, and credentialing management for DOD military, civilian, and contractors. NBIS will serve as the full implementation of the government-wide policy to overhaul the personnel vetting process known as Trusted Workforce 2.0.

National Counterintelligence and Security Center (NCSC): The NCSC is part of the Office of the Director of National Intelligence (ODNI) and is staffed by senior counterintelligence (CI) and other specialists from across the national intelligence and security communities. The NCSC develops, coordinates, and produces: (1) National Threat Identification and Prioritization Assessment and other analytic CI products; (2) The National CI Strategy of U.S. (3) Priorities for CI collection, investigations, and operations; (4) CI program budgets and evaluations that reflect strategic priorities; (5) In-depth espionage damage assessments; and (6) CI awareness, outreach, and training standards policies.

National Industrial Security Program (NISP): National program established by Executive Order (EO) 12829 for the protection of information classified under EO 12958 as amended, or its successor or predecessor orders, and the Atomic Energy Act of 1954, as amended. The National Security Council (NSC) is responsible for providing overall policy direction for the NISP. The Secretary of Defense is the Executive Agent for the NISP. The Information Security Oversight Office (ISOO) is responsible for implementing and monitoring the NISP and for issuing implementing directives that shall be binding on agencies.

National Industrial Security Program Operating Manual (NISPOM): The NISPOM establishes requirements for the protection of classified information disclosed to or developed by contractors, licensees, grantees, or certificate holders to prevent unauthorized disclosure. The 32 Code of Federal Regulations Part 117, "National Industrial Security Program Operating Manual," provides relevant information on oversight of the National Industrial Security Program (NISP). The 32 CFR Part 117, or NISPOM Rule, replaced the NISPOM previously issued as a DOD policy (DOD 5220.22-M) on Feb. 24, 2021.

National Insider Threat Task Force (NITTF): National Task Force focused on Insider Threat issues under joint leadership of the Attorney General and the Director of National Intelligence; established in accordance with Executive Order (EO) 13587, October 2011. The National Counterintelligence Executive (NCIX) and FBI co-direct the daily activities of the NITTF.

National Intelligence: All intelligence, regardless of the source from which derived and including information gathered within or outside of the U.S., which pertains, as determined consistent with any guidelines issued by the President, to the interests of more than one department or agency of the Government.

National Security: A collective term encompassing both national defense and foreign relations of the U.S.

National Security Agency (NSA): The U.S.'s cryptologic organization, with responsibility for protecting U.S. national security information systems and collecting and disseminating foreign signals intelligence. Areas of expertise include cryptanalysis, mathematics, computer science, and foreign language analysis.

National Security Council (NSC): A governmental body specifically designed to assist the President in integrating all spheres of national security policy.

National Security Council Intelligence Directive (NSCID): A formal statement of policy by the National Security Council (NSC), binding upon those U.S. Government agencies within the purview of NSC authority.

National Security Crimes: Crimes likely to impact upon the national security, defense, or foreign relations of the United States, including but not limited to espionage, spying, sabotage, treason, and sedition.

Naval Criminal Investigative Service (NCIS): The NCIS is a federal law enforcement organization whose mission is to protect and serve the Navy and Marine Corps. The NCIS core missions include combatting terrorism, counterintelligence, cyber, and felony investigations.

Need-to-know: A criterion used in security procedures that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his or her official duties.

NOFORN: Foreign release marking for classified information meaning: not releasable to foreign nationals without the permission of the originator.

O==========

Open Source: Any person or group that provides information without the expectation of privacy—the information, the relationship, or both is not protected against public disclosure.

Open Source Intelligence (OSINT): Open source intelligence gathers information that is legally and publicly available, including information from the news media and internet.

Operations Security (OPSEC): A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries and determine which of these represent an unacceptable risk; and then select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level.

P==========

Periodic Reinvestigation (PR): A national security investigation conducted to update a previously completed investigation on persons holding a national security position or performing national security duties to determine whether that individual continues to meet national security requirements.

Personal Contact: As a method of contact, person-to-person contact via any means where the foreign actor, agent, or co-optee is in direct or indirect contact with the target.

Personally Identifiable Information (PII): Information used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, home phone numbers, other demographic, personnel, medical, and financial information. PII includes any information that is linked or linkable to a specified individual, alone, or when combined with other personal or identifying information.

Personnel Security (PERSEC): The security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information or assignment in sensitive positions.

Personnel Security Investigation (PSI): An inquiry into the activities of an individual, designed to develop pertinent information pertaining to trustworthiness and suitability for a position of trust as related to loyalty, character, emotional stability, and reliability.

Phishing Operation: A method of contact. Emails with embedded malicious content or attachments for the purpose of compromising a network to include but not limited to spear phishing, cloning, and whaling.

Physical Security: The security discipline concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

Placement and Access (P&A): An individual's proximity to and ability to collect information of intelligence interest.

Privacy Act: The Privacy Act of 1974 (5 USC §552a) establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.

Program Protection: The safeguarding of defense systems and Technical Data (TD) anywhere in the acquisition process, to include the technologies being developed, the support systems (e.g., test and simulation equipment), and research data with military applications.

Program Protection Plan (PPP): A risk-based, comprehensive, living plan to guide efforts for managing the risks to critical program information (CPI) and mission-critical functions and components.

Publicly Available Information (PAI): Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on- line or otherwise to the public, is available to the public by subscription or purchase, could lawfully be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any vent that is open to the public.

R==========

Research, Development, and Acquisition (RDA): All activities associated with research and engineering, acquisition, international transfers of technology, and disposal of defense-related technology.

Restricted Area: An area (land, sea, or air) in which there are special restrictive measures employed to prevent or minimize incursions and/or interference, where special security measures are employed to prevent unauthorized entry. Restricted areas may be of different types depending on the nature and varying degree of importance of the security interest, or other matter contained therein.

Résumé Academic: A method of contact. Résumé or curricula vitae (CV) submissions for academic purposes.

Résumé Professional: A method of contact. Résumé or curricula vitae (CV) submissions for professional purposes (e.g., seeking a position with a cleared company).

Résumé Submission: A method of operation. Foreign persons submitting résumés for academic or professional placement that would facilitate access to protected information to enable technological or economic advancements by the foreign entity.

Request for Information (RFI) /Solicitation: A method of operation. Collecting protected information by directly or indirectly asking or eliciting personnel for protected information and technology.

Risk: Probability and severity of loss linked to threats or hazards and vulnerabilities.

Risk Analysis: A method by which individual vulnerabilities are compared to perceived or actual security threat scenarios in order to determine the likelihood of compromise of critical information.

Risk Assessment: A systematic examination of risk using disciplined processes, methods, and tools. A risk assessment provides an environment for decision makers to evaluate and prioritize risks continuously and to recommend strategies to remediate or mitigate those risks.

S==========

Sabotage: An act or acts with the intent to injure or interfere with or obstruct the national defense of a country by willfully injuring, destroying, or attempting to destroy any national defense or war materiel, premises, or utilities, to include human or natural resources, under reference.

Search/Seizure: A method of operation. Temporarily accessing, taking, or permanently dispossessing someone of property or restricting freedom of movement via tampering or physical searches of persons, environs, or property.

Secret: Secret information is information or material of which unauthorized disclosure could reasonably be expected to cause serious damage to the national security that the Original Classification Authority (OCA) is able to identify or describe.

SECRET Internet Protocol Router Network (SIPRNet): The worldwide SECRET- level packet switch network that uses high-speed internet protocol routers and high- capacity Defense Information Systems Network circuitry.

Security: A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to

its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Security Classification: A category to which national security information and material is assigned to denote the degree of damage that unauthorized disclosure would cause to national defense or foreign relations of the U.S. and to denote the degree of protection required.

Security Classification Guide (SCG): A documentary form of classification guidance issued by an Original Classification Authority (OCA) that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

Security Clearance: An administrative determination by competent authority that an individual is eligible, from a security stand-point, for access to classified information.

Security Clearance Investigation: An inquiry into an individual's loyalty, character, trustworthiness, and reliability to ensure that he or she is eligible for access to national security information.

Security Compromise: The disclosure of classified information to persons not authorized access thereto.

Security Incident: A security compromise, infraction, or violation.

Security-in-Depth: A determination made by the Cognizant Security Agency (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. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System (IDS), random guard patrols throughout the facility during nonworking hours, closed circuit video monitoring, or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during nonworking hours.

Security Infraction: A security incident that is not in the best interest of security and does not involve the loss, compromise, or suspected compromise of classified information.

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

Security Manager: A properly cleared individual having professional security credentials to serve as the manager for an activity.

Sedition: Willfully advocating or teaching the duty or necessity of overthrowing the U.S. government or any political subdivision by force or violence.

Self-radicalization: Significant steps an individual takes in advocating or adopting an extremist belief system for the purpose of facilitating ideologically-based violence to advance political, religious, or social change. The self-radicalized individual has not been recruited by and has no direct personal

influence or tasking from other violent extremists. The self-radicalized individual may seek out direct or indirect contact with other violent extremists for moral support and to enhance his or her extremist beliefs.

Sensitive: An agency, installation, person, position, document, material, or activity requiring special protection from disclosure that could cause embarrassment, compromise, or threat to the security of the sponsoring power.

Sensitive Activities: Operations, actions, activities, or programs that, if compromised, could have enduring adverse effects on U.S. foreign policy, DOD activities, or military operations or cause significant embarrassment to the U.S., its allies, or the DOD. These are generally handled through special access, compartmented, or other sensitive control mechanisms.

Sensitive Compartmented Information (SCI): A subset of classified national intelligence concerning or derived from intelligence sources, methods or analytical processes that is required to be protected within formal access control systems established by the director or National Intelligence (DNI).

Sensitive Compartmented Information Facility (SCIF): An accredited area, room, group of rooms, or installation where sensitive compartmented information may be stored, used, discussed, and/or electronically processed, where procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular sensitive compartmented information authorized for use or storage within the sensitive compartmented information facility.

Sensitive Information: Information that the loss, misuse, unauthorized access, or modification could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under U.S. Code.

SF 86: The standard form that the DOD uses for most national security background investigations. The automated version of the SF 86 is the Electronic Questionnaires/Applications for Investigations Processing (e-QIP).

Signals Intelligence (SIGINT): Signals Intelligence involves the collection of electronic signals, including phone calls and emails.

Single Scope Background Investigation (SSBI): Investigation for individuals requiring a top secret clearance or working in a critical sensitive position; normally covers a 5-year period and consists of a subject interview, National Agency Check, credit checks, character references, and employment records checks and references.

Social Engineering: An attempt to trick someone into revealing information that can be used to attack systems or networks

Social Networking Service: As a method of contact, contact initiated via a social or professional networking platform.

Special Access Program (SAP): A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Spy: A generic term that refers to either a professional intelligence officer who works for an intelligence service or to a foreign source or asset who steals secrets on behalf of that intelligence service.

Subversion: An act or acts inciting military or civilian personnel of the DOD to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent thereby to interfere with or impair the loyalty, morale, or discipline of the Military Forces of the U.S.

Supply Chain: The linked activities associated with providing materiel from a raw material stage to an end user as a finished product.

Supply Chain Risk Management (SCRM): The management of supply chain risk whether presented by the supplier, the supplied product and its sub-components, or the supply chain (e.g., packaging, handling, storage, and transport).

Surveillance: A method of operation. Systematically observing equipment, facilities, sites, or personnel associated with contracts via visual, aural, electronic, photographic, or other means to identify vulnerabilities or collect information.

Suspicious Contacts: Contractors will report information pertaining to suspicious contacts with employees determined to be eligible for access to classified information, and pertaining to efforts to obtain illegal or unauthorized access to the contractor's cleared facility by any means, including 1) efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information; and 2) efforts by any individual, regardless of nationality, to elicit information from an employee determined eligible for access to classified information, and any contact which suggests the employee may be the target of an attempted exploitation by an intelligence service of another country.

Suspicious Contact Reports (SCR): Reporting concerning suspicious contacts.

T==========

Technology Control Plan (TCP): A detailed plan to control access by foreign national employees and by foreign national visitors on an extended visit authorization at a DOD cleared contractor facility. The TCP stipulates how a company will control access to its export- controlled technology.

Telephone: As a method of contact, contact initiated via a phone call by an unknown or unidentified entity.

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.

Theft: A method of operation. Acquiring protected information with no pretense or plausibility of legitimate acquisition.

Threat Advisory. An advisory is a one-time product or produced on a recurring schedule – daily, weekly, or monthly. The advisory informs authorized recipients of an immediate or the potential for a foreign intelligence or terrorist threat. The advisory typically contains information of a perishable nature.

Threat Indicator: Any observable action that displays violent behavior, abnormal disgruntlement, radicalization, or an extreme world view on religion or another type of ideology.

Top Secret: Top Secret information is information or material of which unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe.

Trade Secret: All forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if: (a) the owner thereof has taken reasonable measures to keep such information secret; and (b) the information derives independent economic value, actual or potential, from not being generally known to and not being readily ascertainable through proper means by the public.

Treason: Whoever, owing allegiance to the U.S, levies war against them or adheres to their enemies, giving them aid and comfort within the U.S. or elsewhere, is guilty of treason.

Trusted Workforce 2.0 (TW 2.0): TW 2.0 is a whole-of-government background investigation reform effort overhauling the personnel vetting process by creating one government-wide system that allows reciprocity across organizations. This includes moving from periodic reinvestigations every five -10 years towards a Continuous Vetting (CV) program, which protects the trusted workforce in real time.

U==========

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

U.S. Air Force Office of Special Investigations (OSI or AFOSI): The U.S. Air Force OSI is a U.S. federal law enforcement agency that reports directly to the Office of the Secretary of the Air Force. AFOSI provides independent criminal investigative counterintelligence (CI) and protective service operations outside of the traditional military chain of command.

U.S. Army Intelligence and Security Command (INSCOM): The U.S. Army Intelligence and Security Command (INSCOM) conducts intelligence, security, and information operations for military commanders and national decision makers.

U.S. Immigration and Customs Enforcement (ICE): ICE's primary mission is to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing boarder control and customs services.

U.S. Munitions List (USML): A list of articles, services, and related technology designated as defense- and space-related by the U.S. federal government.

U.S. Person (USPERS; also USP): A U.S. citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments.

V==========

Vault: A room(s) used for the storing, handling, discussing, and/or processing of SAP information and constructed to afford maximum protection against unauthorized entry.

Vetting: A generic term to describe the full spectrum of asset evaluation for authenticity, reliability, and hostile control. It includes ops testing, case officer and psychological assessment, polygraph, security, counterintelligence interview, production review, and personal record questionnaires.

Violent Extremism: Individuals who openly express their religious, political, or ideological views through violence or a call for violence.

Vulnerability Assessment (VA): A DOD, command, or unit-level evaluation (assessment) to determine the vulnerability of an installation, unit, exercise, port, ship, residence, facility to a terrorist attack.

W==========

Weapons of Mass Destruction (WMD): Chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties and excluding the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon.

Web Form: As a method of contact, contact initiated via a company-hosted web submission form.

Workplace Violence: Any act of violent behavior, threats of physical violence, harassment, intimidation, bullying, verbal or non-verbal threat, or other threatening, disruptive behavior that occurs at or outside the work site.