

## Glossary

# Thwarting the Enemy: Providing Counterintelligence and Threat Awareness Information to the Defense Industrial Base

---

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

**Anomaly:** Foreign power activity or knowledge suggesting foreign knowledge of U.S. national security information, processes or capabilities.

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

**Central Intelligence Agency (CIA):** An independent US Government agency responsible for providing national security intelligence to senior US policymakers. Primary mission: collect, analyze, evaluate, and disseminate foreign intelligence to assist the President and senior U.S. government policymakers in making decisions relating to national security.

**Classified Information:** Information requiring protection in the interest of national security, classified "TOP SECRET, SECRET, or CONFIDENTIAL" according to reference (DCID 1/20; Director of Central Intelligence Directive 1/20, Security, Policy Concerning Travel and Assignment of Personnel With Access to Sensitive Compartmented Information (SCI), December 29, 1991).

**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). There are approximately 8500 cleared contractors with over 13,000 facilities.

**Cleared Defense Contractor (CDC):** A subset of contractors cleared under the NISP who have contracts with the Department of Defense. 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.

**Compromise:** An unauthorized disclosure of classified information.

**Confidential:** Confidential information is information or material of which unauthorized disclosure could reasonably be expected to cause **damage** to the national security that the Original Classification Authority 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.

**Controlled Unclassified Information:** Data bearing distribution limitation statements such as "For Official Use Only" in accordance with reference (DoD 5400.7-R; Freedom of Information Act Program, September, 4, 1998) and other information marked under references (DoD Directive 5230.24, Distribution Statements on Technical Documents, March 18, 1987 and DoD 5400.7-R).

**Counterintelligence:** Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, 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. (EO 12333, amended 30 July 2008)

**Counterintelligence Investigations:** Are conducted to prove or disprove an allegation of espionage or other intelligence activities, such as sabotage, assassination, or other national security crimes conducted by or on behalf of a foreign government, organization, or person or international terrorists. CI investigations may establish the elements of proof for prosecution or administrative actions, provide a basis for CI operations, or validate the suitability of personnel for access to classified information. CI investigations are conducted against individuals or groups for committing major security violations, as well as failure to follow Defense Agency and Military Department directives governing reporting contacts with foreign citizens and out-of-channel requests for defense information. CI investigations provide military commanders and policymakers with information used to eliminate security vulnerabilities and otherwise improve the security posture of threatened interests.

**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.

**Defense Criminal Investigation Service (DCIS):** The criminal investigative arm of the Inspector General (IG) of the Department of Defense responsible for investigating: terrorism; technology/munitions theft & diversion; cyber crime; substandard/defective products; and fraud, bribery & corruption.

**Defense Intelligence Agency (DIA):** A Department of Defense combat support agency and a member of the United States Intelligence Community responsible for providing timely, objective, and cogent military intelligence to warfighters, defense planners, and defense and national security policymakers. DIA is a major producer and manager of foreign military intelligence.

**Defense Travel Briefs:** Formal advisories alerting personnel of the potential for harassment, exploitation, provocation, capture, or entrapment while traveling. These briefings, based on actual experience when available, include information on courses of action helpful in mitigating adverse security and personnel consequences and advise of passive and active measures that personnel should take to avoid becoming targets or inadvertent victims as a consequence of hazardous travel.

**Department of Homeland Security (DHS):** A cabinet department of the United States federal government, established on November 25, 2002. 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.

**Departments and agencies:** Refers to any “Executive agency,” as defined in 5 U.S.C. 105; any “Military department” as defined in 5 U.S.C. 102; any “independent establishment,” as defined in 5 U.S.C. 104; and any other entity within the executive branch that comes into the possession of classified information.

**DoD Component CI Organizations:** The organic CI elements of the Army, the Navy, the Air Force, the Marine Corps, the Joint Staff, the Combatant Command Staffs, the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the Defense Security Service, the Defense Threat Reduction Agency, and the Missile Defense Agency and the CIFA.

**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.

**Employee:** For purposes of the National Insider Threat Policy, “employee” has the meaning provided in section 1.1(e) of 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.

**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

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

**Executive Order 12333:** Authorizes elements of the Intelligence Community to collect, retain, or disseminate information concerning United States 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.

**Facility Security Officer (FSO):** The security officer for a cleared defense contractor facility, the FSO supervises and directs security measures necessary for implementing requirements of the National Industrial Security Program and Federal requirements for classified information.

**Foreign Diplomatic Establishment:** Any embassy, consulate, or interest section representing a foreign country.

**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 which may result in unauthorized access to classified information and/or special nuclear material or may affect adversely the performance of classified matters.

**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.

**Federal Bureau of Investigation (FBI):** The FBI has primary responsibility for counterintelligence investigations within the United States.

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

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

**InfraGard:** A partnership between the FBI and the private sector that shares and analyzes threats. InfraGard is an association of individuals, academic institutions, state and local law

enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.

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

**Insider Threat:** The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States 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 IC policy for the protection of national intelligence and provides framework for greater coordination and communications between counterintelligence and security activities of the IC 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 programs across the IC to create a strategic approach to counterintelligence that will enhance the national security posture of the U.S. The ICD 750 recommends counterintelligence to be functionally integrated with security programs per the ICD 700.

**International Traffic in Arms Regulations (ITAR):** The International Traffic in Arms Regulations, or ITAR, implement the provisions of the Arms Export Control Act, or AECA, and control the export and import of defense-related articles and services on the United States Munitions List.

**Lead CI Agency:** A Military Department CI Agency that has been designated by the USD(I) to provide defined levels of CI support to one or more of the DoD Components.

**Military Department CI Agencies:** The Military Department CI Agencies include the U.S. Army Counterintelligence, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations.

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

**National Counterintelligence and Security Center (NCSC):** The NCSC is part of the Office of the Director of National Intelligence and is staffed by senior counterintelligence 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 Counterintelligence Strategy of the U.S. of America; (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 Security:** A collective term encompassing both national defense and foreign relations of the United States.

**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.

**NISPOM:** DoD 5220.22-M, National Industrial Security Program Operating Manual. The NISPOM prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information.

**Open Source Intelligence (OSINT):** Open Source Intelligence gathers information that is legally and publically 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; then select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level.

**Portico:** A program managed by the CIFA to provide automation support, through web-enabled software hosted on a robust infrastructure, to the DoD CI Community. Portico enables CI enterprise business processes; facilitates information sharing and coordination across DoD Services and Agencies; and provides management tools for each CI functional area, as well as supporting tools and services for managing the CI process in the functional areas of Collection; Investigations; Analysis and Production; Operations; and CI Functional Services.

**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 (Sections 792-799, Chapter 37 of title 18, United States Code).

**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.

**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 is able to identify or describe

**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.

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

**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.

**Spying:** During wartime, any person who is found lurking as a spy or acting as a spy in or about any place, vessel or aircraft, within the control or jurisdiction of any of the Armed Forces or in or about any shipyard, any manufacturing or industrial plant, or any other place or institution engaged in work in aid of the prosecution of the war by the United States, or elsewhere.

**Subversion:** An act or acts inciting military or civilian personnel of the Department of Defense 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, of discipline, of the Military Forces of the United States.

**Technology Control Plan:** Stipulates how a company will control access to its export-controlled technology

**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.

**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 Original Classification Authority is able to identify or describe

**Treason:** Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason (see Section 2381 of title 18, U.S. Code, reference (Sections 792-799, Chapter 37 of title 18, United States Code).

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

**U.S. Army Intelligence 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. Air Force Office of Special Investigations (OSI):** The United States Air Force OSI is a U.S. federal law enforcement agency that reports directly to the Office of the Secretary of the

Air Force. Operating worldwide, AFOSI provides independent criminal investigative, counterintelligence and protective service operations outside of the traditional military chain of command. AFOSI proactively identifies, investigates and neutralizes, serious criminal, terrorist, and espionage threats to personnel and resources of the U.S. Air Force and the Department of Defense, thereby protecting the national security of the United States.

**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, customs services.