



## Insider Threat Definitions

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

<b>A</b>	
<b>Access</b>	The ability and opportunity to obtain knowledge of classified sensitive information or to be in a place where one could expect to gain such knowledge. NISPOM: The ability and opportunity to gain knowledge of classified information.
<b>Adjudication</b>	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 trustworthy decision.
<b>Advanced Persistent Threat (APT)</b>	An adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of ex-filtrating information; undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future.
<b>Adverse Information</b>	Any information that adversely reflects on the integrity or character of a cleared employee that suggests that his or her ability to safeguard classified information may be impaired, that his or her access to classified information clearly may not be in the interest of national security, or that the individual constitutes as an insider threat.
<b>Adversary</b>	Any individual, group, organization, or government that conducts or has the intent and capability to conduct activities detrimental to the US Government or its assets. Adversaries may include intelligence services, political or terrorist groups, criminals, and private interests.
<b>Adversary Collection Methodology</b>	Any resource and method available to and used by an adversary for the collection and exploitation of sensitive/critical information or indicators thereof.

<b>Agent</b>	An individual who acts under the direction of an intelligence agency or security service to obtain, or assist in obtaining, information for intelligence or counterintelligence purposes.
<b>Air Force Office of Special Investigations (AFOSI)</b>	U.S. Air Force’s major investigative service; a federal law enforcement and investigative agency operating throughout the full spectrum of conflict, seamlessly within any domain; conducting criminal investigations and providing counterintelligence services.
<b>All-Source Analysis</b>	An intelligence activity involving the integration, evaluation, and interpretation of information from all available data sources and types, to include human intelligence, signals intelligence, geospatial intelligence, measurement & signature intelligence, and open source intelligence.
<b>Analysis</b>	The process by which information is transformed into intelligence; systemic examinations of information to identify significant facts, make judgments, and draw conclusions.
<b>Anomalies</b>	See <i>Counterintelligence Anomalies</i>
<b>Anomalous Activity</b>	Irregular or unusual deviations from what is usual, normal, or expected; activity inconsistent with the expected norm. Also, network activities that are inconsistent with the expected norms that may suggest a trusted insider is exploiting access to information for nefarious and illegal activity.
<b>Asset</b>	Person, structure, facility, information, material, or process that has value.
<b>Authorization to Search</b>	An express permission, written or oral, issued by competent military authority, to search a person or an area for specified property or evidence or to search for a specific person and to seize such property, evidence, or person. NISPOM: Authorized Person. A person who has a need-to-know for classified information in the performance of official duties and who has been granted a personnel security clearance at the required level.
<b>B</b>	
<b>Background Investigation (BI)</b>	An official inquiry into the activities of a person designed to develop information from a review of records, interviews of the subject, and interviews of people having knowledge of the subject.
<b>Behavioral Science Consultant</b>	A professional with extensive training in behavioral science, mental health, psychiatry, or psychology.
<b>C</b>	
<b>Central Intelligence Agency (CIA)</b>	An independent agency responsible for providing national security intelligence to senior US policymakers. The Director of the Central Intelligence Agency (D/CIA) is nominated by the president with the advice and consent of the Senate. The Director manages the operations, personnel, and budget of the Central Intelligence Agency. The CIA is separated into five

<b>CIA (con't.)</b>	basic components: the Directorate of Operations, the Directorate of Analysis, the Directorate of Science & Technology, the Directorate of Support, and the Directorate of Digital Innovation. They carry out “the intelligence cycle,” the process of collecting, analyzing, and disseminating intelligence information to top US government officials.
<b>Chain of Custody</b>	A chronological written record reflecting the release and receipt of evidence from initial acquisition until final disposition.
<b>CI Acronym</b>	See <i>Counterintelligence</i> .
<b>Circumstantial Evidence</b>	Evidence that requires interpretation or that requires a judge or jury to reach a conclusion based on what the evidence indicates. From the close proximity of the defendant to a smoking gun, for example, the jury might conclude that she pulled the trigger.
<b>Clandestine Operation</b>	An operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of the identity of the sponsor.
<b>Classification</b>	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.
<b>Classified Information</b>	Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and that which has been so designated. NISPOM: Official information that has been determined, pursuant to EO13526, Classified National Security Information, or any predecessor order, to require protection against unauthorized disclosure in the interest of national security and that which has been so designated.
<b>Clearance</b>	Formal security determination by an authorized adjudicative office that an individual is authorized access, on a need-to-know basis, to a specific level of collateral classified information (TOP SECRET, SECRET, CONFIDENTIAL).
<b>Cleared Contractor (CC)</b>	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.
<b>Cleared Employee</b>	All contractor employees granted personnel clearances and all employees being processed for clearances.
<b>Cleared Defense Contractor (CDC)</b>	A company or academic institution (i.e., university or college) that has entered into a security agreement with the DoD, and was granted a facility (security) clearance enabling the entity to be eligible for access to classified information of a certain category, as well as all lower categories.

<b>Collateral</b>	All national security information classified CONFIDENTIAL, SECRET, or TOP SECRET in accordance with the provisions of an Executive order for which special systems of compartmentation (e.g., SCI or special access programs) are not formally required.
<b>Collection</b>	The exploitation of sources by collection agencies, and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence.
<b>Company</b>	NISPOM: A generic and comprehensive term that may include sole proprietorships, individuals, partnerships, corporations, societies, associations, and organizations usually established and operating to carry out a commercial, industrial, or other legitimate business, enterprise, or undertaking.
<b>Compartmentation</b>	The principle of controlling access to sensitive information so that it is available only to those individuals or organizational components with an official "need-to-know" and only to the extent required for the performance of assigned responsibilities.
<b>Compromised</b>	A term applied to a classified matter. Knowledge of which has, in whole or in part, passed to an unauthorized person or persons or which has been subject to the risk of such passing.
<b>Cyber</b>	Any process, program, or protocol relating to the use of the internet or an intranet, automatic data processor or transmission, or telecommunication via the internet or an intranet; or any matter relating to, or involving the use of, computers or computer networks.
<b>Cybersecurity</b>	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.
<b>Confidential</b>	Security classification that shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.
<b>Continuous Evaluation</b>	Reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information.
<b>Controlled Unclassified Information (CUI)</b>	Unclassified information that does not meet the standards for National Security Classification under Executive Order 12958 but is (1) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (2) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

<b>Counterespionage (CE)</b>	That aspect of counterintelligence designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities.
<b>Counterintelligence (CI)</b>	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.
<b>Counterintelligence Anomalies</b>	Foreign power activity or knowledge, inconsistent with the expected norms that suggest prior foreign knowledge of U.S. national security information, processes, or capabilities.
<b>Counterintelligence Awareness</b>	An individual's level of comprehension as to the FIE (foreign intelligence entity) threat, methods, indicators, and reporting requirements.
<b>Counterintelligence Inquiry</b>	An examination of the facts surrounding an incident of potential CI interest, to determine if a CI investigation is necessary.
<b>Counterintelligence Insider Threat (CI InT)</b>	A person, known or suspected, who uses their authorized access to DoD facilities, personnel, systems, equipment, information, or infrastructure to damage and disrupt operations, compromise DoD information, or commit espionage on behalf of an FIE (Foreign Intelligence Entity).
<b>Counterintelligence Investigation</b>	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.
<b>Counterintelligence Operations.</b>	Proactive activities designed to identify, deceive, exploit, disrupt, neutralize, or deter FIE (Foreign Intelligence Entity) activities.
<b>Counterintelligence Risk Assessment</b>	An assessment that examines threat information and identifies organizational vulnerabilities to make an informed determination about the likelihood and consequence of the loss or compromise of sensitive information and assets to foreign intelligence entities.
<b>Countermeasure</b>	Anything that effectively negates or mitigates an adversary's ability to exploit vulnerabilities.
<b>Countermeasures</b>	The employment of devices and/or techniques that has as its objective the impairment of the operational effectiveness of an adversary's activity. Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities.
<b>Criminal Investigation</b>	Investigation into alleged or apparent violations of law undertaken for purposes that include the collection of evidence in support of potential criminal prosecution.

<b>Critical Asset</b>	A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively.
<b>Critical Infrastructure</b>	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on the security, national economic security, national public health and safety, or any combination of those matters.
<b>Cyber Incident</b>	Any attempted or successful access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or an information system, without lawful authority.
<b>Cybersecurity</b>	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. DoDI 8500.01
<b>Cyber Threats</b>	Natural or man-made incidents (intentional or unintentional) that would be detrimental to the cyber domain, or which are dependent on or operate through cyberspace/cyber domain.
<b>D</b>	
<b>Deception</b>	An action intended by an actor to influence the perceptions, decisions, and actions of another.
<b>Deduction</b>	The process of reasoning from general rules to particular cases. Deduction may also involve drawing out or analyzing premises to form a conclusion.
<b>Defector</b>	A person who has consciously abandoned loyalty to his country and who possess intelligence information of value to another country or countries.
<b>Defense Industrial Base (DIB)</b>	The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements.
<b>Defense Intelligence Agency (DIA)</b>	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.
<b>Defense Security Enterprise (DSE)</b>	The organizations, infrastructure, and measures (including policies, processes, procedures, and products) in place to safeguard DoD personnel, information, operations, resources, technologies, and facilities against harm, loss, or hostile acts and influences. This system of systems comprises personnel, physical, industrial, information, operations, and SAP security policy, critical program information and protection policy, and security training. It addresses, as part of information security,

<b>DSE (Con't.)</b>	classified information, including sensitive compartmented information and controlled unclassified information. It aligns with CI, information assurance, foreign disclosure, security cooperation, technology transfer, export control, cyber security, nuclear physical security, chemical and biological security, antiterrorism, force protection, and mission assurance policy and is informed by other security related efforts.
<b>Defense Security Service (DSS)</b>	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, 24 federal agencies, and approximately 13,000 cleared contractor facilities with security support services.
<b>Department of State / Bureau of Diplomatic Security (DS)</b>	The security and law enforcement arm of the U.S. Department of State. DS is responsible for providing a safe and secure environment for the conduct of U.S. foreign policy; it is involved in international investigations, threat analysis, cyber security, counterterrorism, security technology, and protection of people, property, and information.
<b>Deterrence</b>	The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction.
<b>Disgruntled Employee</b>	An employee who may be annoyed, discontent, displeased, dissatisfied, grumpy, irritated, malcontent, or upset to the point that he may take violent action against a coworker, supervisor, or employer.
<b>Disguise</b>	Concealment or misrepresentation of the physical characteristics or true nature or identity of a person or object.
<b>Dissemination</b>	The transmission, communication, sharing, or passing of information outside a Defense Intelligence Component by any means, including oral, electronic, or physical means. Dissemination includes providing any access to information in a Component's custody to persons outside the Component.
<b>Divided Loyalties</b>	Broadly defined individuals with intellectual or emotional commitments to another country through cultural affinity.
<b>DoD Criminal Investigative Organizations</b>	The term refers collectively to the United States Army Criminal Investigation Command, Naval Criminal Investigative Service, U.S. Air Force Office of Special Investigations, and Defense Criminal Investigative Service, Office of the IG DoD.
<b>DoD Insider Threat Management and Analysis Center (DITMAC)</b>	A cross-functional team of analysts that aggregates, integrates reviews, analyzes, and shares information that is indicative of a potential insider threat. The DITMAC will exercise this information management capability with the ability to assess risk; refer issues for further consideration, investigation, and potential action; synchronize responses; and oversee resolution of identified issues across the Department within DoD-approved resources.

<b>DoD Law Enforcement Agencies</b>	Organizations, agencies, entities, and offices of the Military Departments and Defense Agencies and the Inspector General of the Department of Defense that perform an LE (law enforcement) function for those departments and agencies and are manned by DoD LEOs [Law Enforcement Officers].
<b>Due Process</b>	A right guaranteed by the Fifth, Sixth, and Fourteenth Amendments of the U.S. Constitution and generally understood, in legal contexts, to mean the due course of legal proceedings according to the rules and forms established for the protection of individual rights. In criminal proceedings, due process of law is generally understood to include the following basic elements: a law creating and defining the offense, an impartial tribunal having jurisdictional authority over the case, accusation in proper form, notice and opportunity to defend, trial according to established procedure, and discharge from all restraints or obligations unless convicted.
<b>E</b>	
<b>Economic Espionage</b>	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.
<b>Enterprise Risk Standards</b>	Standards surrounding behavioral indicators, component reporting requirements, and the model that drives scoring and analysis to identify potential insider threats.
<b>Elicitation</b>	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.
<b>Espionage</b>	Intelligence activity directed towards the acquisition of information through clandestine means.
<b>Espionage Indicators</b>	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.
<b>(Potential) Espionage Indicators</b>	Activities, behavior, or circumstances that may, unless satisfactorily explained, be indicative of potential espionage activity by an individual who may be acting as a witting espionage agent or spy.
<b>(Potential) Risk Indicators</b>	Activities, behavior, or circumstances that may be indicative of increased insider threat risk.
<b>Evidence</b>	Testimonies, writings, material objects, or other things presented to the senses that are offered to prove the existence or nonexistence of a fact. In the broadest sense, evidence consists of all matters that are logically relevant to the resolution of any issue of concern.



<b>Executive Order (EO) 12333</b>	Executive order that provides both an overarching framework and specific rules governing U.S. intelligence activities; full title is Executive Order 12333 United States Intelligence Activities.
<b>Exploitation</b>	The process of obtaining information from any source and taking advantage of it.
<b>F</b>	
<b>FIE</b>	Acronym; see <i>Foreign Intelligence Entity</i> .
<b>FIS</b>	Acronym for Foreign Intelligence Service; see <i>Foreign Intelligence and Security Service</i> .
<b>Federal Bureau of Investigation (FBI)</b>	The primary investigative arm of the US Department of Justice (DoJ) with jurisdiction over violations of more than 200 categories of federal law and also a statutory member of the US Intelligence Community. The FBI's mission is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.
<b>Foreign Collection Threat</b>	Opportunity for a foreign entity or cooperating DoD personnel (an insider) to overtly, covertly, or clandestinely collect information about RDA programs, technologies, system capabilities, and employment methods that may enable an adversary to copy, counter, or defeat a capability, or inhibit, exploit, or sabotage a defense system. Within the context of DoDI O-5240.24, the term collectively refers to threats posed by or from an insider, cyber exploitation, supply chain manipulation, an FIE (foreign intelligence entity), a foreign company, international transfers, or exports of technology, and disposal of export-controlled technology.
<b>Foreign Intelligence Entity (FIE)</b>	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 [FISS] and international terrorist organizations.
<b>Foreign Ownership, Control, or Influence (FOCI)</b>	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 and/or special nuclear material or may affect adversely the performance of classified matters.
<b>Foreign Travel Brief</b>	A tailored briefing provided to personnel traveling outside the United States to increase the traveler's awareness of: 1) personal safety; 2) potential targeting by foreign intelligence; 3) travel warnings & alerts; and 4) where to seek assistance in an emergency.

<b>Foreign Visit</b>	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.
<b>Full-Field Counterintelligence Investigation</b>	An investigation in which there is a reasonable belief a member of the U.S. military; a civilian employee or contractor of DoD; or an individual having access to DoD installations, personnel, or information is engaged in spying or has committed or attempted to commit espionage, sabotage, treason, sedition, subversion, assassination, or international terrorist activity or otherwise poses a threat to national security.
<b>H</b>	
<b>Hacker</b>	Unauthorized user who attempts to or gains access to an information system.
<b>Honey Trap</b>	The term universally applied to operations undertaken to ensnare an unwary target in a compromising sexual encounter that may leave the victim vulnerable to blackmail that might result in espionage.
<b>I</b>	
<b>IG</b>	The criminal investigative arm of the Inspector General(IG) of the Department of Defense responsible for investigating: terrorism; technology/munitions theft & diversion; cybercrime; substandard/defective products; and fraud, bribery & corruption.
<b>Illegal</b>	An intelligence officer or a recruited agent who operates in a foreign country in the guise of a private person, and is often present under a false identity.
<b>Indicator</b>	Data derived from friendly detectable actions and open-source information that adversaries can interpret and piece together to reach conclusions or estimates of critical or classified information concerning friendly intentions, capabilities, or activities.
<b>Industrial Espionage</b>	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.
<b>Industrial Security</b>	That portion of information security that is concerned with the protection of classified information in the custody of U.S. industry.
<b>Information Assurance (IA)</b>	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Committee on National Security Systems Instruction No. 4009, April 26, 2010.

<b>Information Security</b>	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, statute, or regulation. Information security includes protection of classified, controlled unclassified, and sensitive compartmented information.
<b>Inquiry</b>	The initial fact-finding and analysis process to determine the facts of any security incident.
<b>Insider</b>	DoDD 5205.16: Any person with authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD. NISPOM DoD 5220.22-M: Cleared contractor personnel with authorized access to any Government or contractor resource, including personnel, facilities, information, equipment, networks, and systems.
<b>Insider Threat (InT)</b>	DoDD 5205.16: The threat an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This 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. NISPOM DoD 5220.22-M: The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information.
<b>Insider Threat Hub</b>	A centralized multi-disciplinary staff element or activity established by a component that possesses an integrated capability to monitor, audit, fuse, and analyze incoming information for insider threat detection and mitigation. Hub personnel will be able to analyze information and activity indicative of an insider threat and refer that data to the appropriate officials to investigate or otherwise resolve.
<b>Intelligence Activities</b>	All activities that elements of the Intelligence Community are authorized to conduct pursuant to Executive Order 12333.
<b>Intelligence Community (IC)</b>	All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role.
<b>L</b>	
<b>Law Enforcement</b>	The generic name for the activities of the agencies responsible for maintaining public order and enforcing the law, particularly the activities of preventing, detecting, and investigating crime and apprehending criminals.

<b>Lawful Search</b>	An examination, authorized by law, of a specific person, property, or area for specified property evidence, or a specific person, for the purpose of seizing such property, evidence, or person.
<b>Leaks</b>	Jargon for unauthorized disclosures.
<b>Least Intrusive Means</b>	The collection of information about US persons shall be accomplished by the <i>least intrusive means</i> .
<b>M</b>	
<b>Malicious Code</b>	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host.
<b>Malicious Cyber Activity</b>	Activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information, or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.
<b>Malware</b>	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
<b>Media Exploitation</b>	The receipt, cataloging, duplication, screening/prioritizing, listing, initial evaluation, translating key pieces of media, uploading data into appropriate data bases, identifying the need for further detailed exploitation of pieces of media, tracking the requested detailed exploitation efforts, and disseminating selected media for further use/analysis by the Intelligence Community.
<b>Military Intelligence (MI)</b>	Collection, analysis, production, and dissemination of information relating to any foreign military or military-related situation or activity that is significant to military policy-making or the planning and conduct of military operations and activities.
<b>Miranda Warnings</b>	The advisement of rights due criminal suspects by the police before questioning begins.
<b>Mitigation</b>	Ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident. Includes solutions that contain or resolve risks through analysis of threat activity and vulnerability data, which provide timely and accurate responses to prevent attacks, reduce vulnerabilities, and fix systems.
<b>Modus Operandi (MO)</b>	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.
<b>Mole</b>	A member of an organization who is spying and reporting on his/her own organization on behalf of a foreign country; also called a penetration.

N

<b>National Agency Check (NAC)</b>	An in-depth name trace consisting of Federal Bureau of Investigation Name and Criminal History Fingerprint Checks, Defense Clearance Investigation Index (DCII) search, and can include checks on military personnel records, citizenship, selective service, Central Intelligence Agency records, State Department records, and other US Government agencies.
<b>National Insider Threat Task Force (NITTF)</b>	National Task Force focused on Insider Threat issues under joint leadership of the Attorney General and the Director of National Intelligence, established IAW EO 13587, October 2011. The NCIX and FBI co-direct the daily activities of the NITTF.
<b>Naval Criminal Investigative Service (NCIS)</b>	The federal law enforcement agency charged with conducting investigations of felony-level offenses affecting the Navy and Marine Corps – that is, crimes punishable by confinement for more than one year. NCIS also performs investigations and operations aimed at identifying and neutralizing foreign intelligence, international terrorists, and cyber threats to the Department of the Navy. In addition, it provides warning of threats and specialized defensive force protection support to U.S. naval forces around the world. Criminal investigation is at the foundation of virtually all what the organization does, but the NCIS mission is broad. Transnational terrorism has been and remains a key focus area for the agency.
<b>Need-to-know</b>	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. NISPOM: A determination made by an authorized holder of classified information that a prospective recipient has a requirement for access to, knowledge, or possession of the classified information to perform tasks or services essential to the fulfillment of a classified contract or program.
<b>Network</b>	In critical infrastructure protection usage, a group or system of interconnected or cooperating entities, normally characterized as being nodes (assets), and the connections that link them.
<b>NOFORN</b>	Foreign release marking for classified information meaning: “not releasable to foreign nationals without the permission of the originator.”
<b>Non-Disclosure Agreement (NDA)</b>	An official authorized contract between an individual and the United States (U.S.) Government, signed by an individual as a condition of access to classified national intelligence. The NDA specifies the security requirements for access and details the penalties for noncompliance.

O

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

P	
<b>Pattern Recognition</b>	An inductive process of recognizing a commonality or trend in an aggregate of indications from which a plausible explanation or model can be developed.
<b>Patterns</b>	Repeated incidents that may be similar in nature or dissimilar events that occur in a specific location or time span that may indicate a potential insider threat.
<b>Penetration</b>	In intelligence usage, the recruitment of agents within or the infiltration of agents or technical monitoring devices in an organization or group for the purpose of acquiring information or of influencing its activities.
<b>Personally Identifiable Information (PII)</b>	Information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual. Includes information about an individual that identifies, links, relates, or is unique to or describes him or her (e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home or office phone numbers; other demographic, biometric, personnel, medical, and financial information; etc.).
<b>Personnel Security</b>	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.
<b>Potential Espionage Indicators</b>	See Espionage Indicators.
<b>Potential Risk Indicators</b>	An action, event, or condition that precedes the insider act and is hypothesized to be associated with the act. The observable precursors contribute to increased risk.
<b>Physical Search</b>	Any intrusion on a person or a person's property or possessions for the purpose of obtaining property, information, or stored electronic data or communications, and that would require a warrant for law enforcement purposes. A physical search includes an intrusion that violates a reasonable expectation of privacy or that involves a trespass or otherwise physically occupying private property. It also includes the examination of the interior of property or the scan of a person by technical means. The law in this area is subject to change, and a Defense Intelligence Component should consult with the legal office responsible for advising it on those activities that may constitute a physical search.
<b>Placement</b>	An individual's proximity to information of intelligence interest.
<b>Placement and Access (P&amp;A)</b>	An individual's proximity to and ability to collect information of intelligence interest.
<b>Polygraph and Credibility Assessment (PCA)</b>	The overarching term covering programs, research, training, and procedures that employ technologies to assess an individual's truthfulness with the aid of technical devices that measure physiological data or behavioral activity.

<b>Preliminary Inquiry</b>	An unobtrusive review of the facts and circumstances of an incident or allegation to determine if the preliminary information or circumstances is sufficient to warrant the initiation of an investigation or referral to an investigative entity. The limited objective will be determined by the policy of individual agencies and may include the collection of information from other agencies and/or other records such as travel, financial, HR, security, and badging [sic], etc., which may be used to make an informed determination if the incident involved is part of a pattern.
<b>Privacy Act</b>	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. A system of records is a group of records under the control of an agency from which information is retrieved by an individual's name or by some other identifier assigned to the individual. The Privacy Act requires that agencies provide public notice of their systems of records through publication in the Federal Register. The Privacy Act prohibits the disclosure of information from a system of records absent the written consent of the individual who is the subject of the information search, unless the disclosure is pursuant to one of 12 statutory exceptions.
<b>Probable Cause</b>	When reasonable grounds exist to believe that an offense has been or is being committed and the person to be apprehended committed or is committing it.
<b>Proliferation</b>	The transfer of weapons of mass destruction, related materials, technology, and expertise from suppliers to hostile state or non-state actors.
<b>R</b>	
<b>Radicalization</b>	The social and behavioral process whereby people adopt and embrace extremist attitudes, values, or behaviors. It is a risk factor for involvement in terrorism, but involvement in terrorism does not always result from radicalization.
<b>Reasonable Suspicion</b>	A belief based on facts that would lead a reasonable person to conclude, in light of his or her experience, that criminal activity may be afoot.
<b>Records Check</b>	The process whereby an Insider Threat program official obtains relevant information about Sources or Subjects from the records and information holdings of military, civilian, or government agencies, as well as certain commercial companies and vendors during the conduct of a preliminary inquiry.
<b>Recruitment</b>	The deliberate and calculating effort to gain control of an individual and to induce him or her to furnish information or to carry out intelligence tasks for an intelligence or CI service.
<b>Remediation</b>	Actions taken to correct known deficiencies and weaknesses once vulnerability has been identified.

<b>Reportable Incident</b>	Any suspected or alleged violation of policy or of other related orders, policies, procedures or applicable law, for which there is credible information.
<b>Reporting Requirements</b>	Requirements, codified in DoD policy, that dictate what information Components must report to DITMAC. These requirements will be developed through collaboration among DITMAC, Component, and USD(I) representatives, and will evolve over time.
<b>Risk</b>	A measure of consequence of peril, hazard, or loss, which is incurred from a capable aggressor or the environment (the presence of a threat and unmitigated vulnerability).
<b>Risk Analysis</b>	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.
<b>Risk Assessment</b>	Assessments that provide decision makers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgements concerning the extent of actions needed to reduce risk. They provide a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies. Risk assessments generally include the tasks of identifying threats and vulnerabilities and determining consequences.
<b>Risk Management (RM)</b>	The process of identifying, assessing, and controlling, risks arising from operational factors and making decisions that balance risk cost with mission benefits.
<b>Risk Mitigation</b>	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.
<b>Rule of the Least Intrusive Means</b>	The collection of information by a DoD intelligence component must be accomplished by the <b>least intrusive means</b> or lawful investigative technique reasonably available.
<b>S</b>	
<b>Sabotage</b>	An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war materiel, premises, or utilities, to include human and natural resources.
<b>Search</b>	An examination, authorized by law, of a specific person, property, or area for specified property or evidence, or for a specific person for the purpose of seizing such property, evidence, or person.
<b>Search Warrant</b>	A document issued by a judicial officer that directs a law enforcement officer to conduct a search at a specific location, for specified property or person relating to a crime, to seize the property or person if found, and to account for the results of the search to the issuing judicial officer.



<b>Secret</b>	Security classification that shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
<b>Section 603 Referral</b>	Section 603 of the "Intelligence Authorization Act for FY 1990" states: "Subject to the authority of the Attorney General, the FBI shall supervise the conduct of all investigations of violations of the espionage laws of the United States by persons employed by or assigned to United States diplomatic missions abroad. All departments and agencies shall report immediately to the FBI any information concerning such a violation. All departments and agencies shall provide appropriate assistance to the FBI in the conduct of such investigations. Nothing in this provision shall be construed as establishing a defense to any criminal, civil, or administrative action."
<b>Section 811 Referral</b>	Section 811 of the Intelligence Authorization Act of 1995 (50 USC §402a) is the legislative act that governs the coordination of counterespionage investigations between Executive Branch agencies and departments and the FBI. Section 811 referrals are the reports – made by the Executive Branch agencies or departments to the FBI under Section 811(c)(1)(a) – that advise the FBI of any information, regardless of origin, which may indicate that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or agent of a foreign power.
<b>Security</b>	Proactive measures adopted to safeguard personnel, information, operations, resources, technologies, facilities, and foreign relations against harm, loss, or hostile acts and influences.
<b>Security Classification Guide (SCG)</b>	A documentary form of classification guidance issued by an OCA (original classification authority) 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.
<b>Security Clearance</b>	An administrative determination by competent authority that an individual is eligible, from a security stand-point, for access to classified information.
<b>Security Clearance Investigation</b>	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.
<b>Security Compromise</b>	The disclosure of classified information to persons not authorized access thereto.
<b>Security Countermeasures (SCM)</b>	Actions, devices, procedures, and/or techniques to reduce security risks.
<b>Security Incident</b>	A security compromise, infraction, or violation.
<b>Security Infraction</b>	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.
<b>Security Manager</b>	A properly cleared individual having professional security credentials to serve as the manager for an activity.

<b>Security Measures</b>	Actions taken by the government and intelligence departments and agencies, among others, for protection from espionage, observation, sabotage, annoyance, or surprise. With respect to classified materials, it is the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national defense.
<b>Seizure</b>	The taking or dispossession of property from the possessor by an authorized person or the restriction of the freedom of movement of an individual against his or her will by an agent of the Government.
<b>Self-radicalization</b>	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 (through the internet for example) contact with other violent extremists for moral support and to enhance his or her extremist beliefs.
<b>Senior official</b>	The DoD official, designated by a DoD Component head, responsible for the direction, management, and oversight of the component's insider threat program.
<b>Social Engineering</b>	The act of manipulating people into performing actions or divulging confidential information. It relies on human interactions, such as trying to gain the confidence of someone through trickery or deception for the purpose of information gathering, fraud, or computer system access. This can take many forms, both online and offline.
<b>Social Media</b>	Web-based tools, websites, applications, and media that connect users and allow them to engage in dialogue, share information, collaborate, and interact. Social media websites are oriented primarily to create a rich and engaging user experience. In social media, users add value to the content and data online; their interactions with the information (e.g., both collectively and individually) can significantly alter the experiences of subsequent users.
<b>Steganography</b>	The art, science, and practice of communicating in a way that hides the existence of the communication.
<b>Subject</b>	Person, place, or thing observed or is under investigation.
<b>Suspect</b>	An adult or a juvenile who has not been arrested or charged but whom a criminal justice agency believes may be the person responsible for a specific criminal offense.
<b>Suspect</b>	A person, corporation, or other legal entity about which some credible information exists to believe that the person or entity committed a particular criminal offense.
<b>T</b>	
<b>Threat</b>	An adversary having the intent, capability, and opportunity to cause loss or damage.

<b>Threat Analysis.</b>	A process that examines an adversary’s technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities.
<b>Threat Assessment</b>	A resultant product of the defined process used to conduct a threat analysis and develop an evaluation of a potential threat.
<b>Trade Secret</b>	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.
<b>Trade Secret Theft</b>	Defined under §1832 of the Economic Espionage Act of 1996 and covers the conversion of a trade secret to the economic benefit of anyone other than the rightful owner. There is no requirement for a foreign nexus in Trade Secret Theft.
<b>U</b>	
<b>Unauthorized Disclosure</b>	A communication or physical transfer of classified information to an unauthorized recipient.
<b>V</b>	
<b>Violent Behavior</b>	The intentional use of physical force or power, threatened or actual, against a person or group that either results in or has a high likelihood of injury, death, or psychological harm to self or others.
<b>Violent Extremism</b>	Individuals who openly express their religious, political, or ideological views through violence or a call for violence. Also, any ideology that encourages, endorses, condones, justifies, or supports the commission of a violent act or crime to achieve political, social, or economic changes.
<b>Vulnerability</b>	Weakness in an information system, system security procedures, internal controls, physical or technical access controls, or implementation that could be exploited by a threat source; open to attack, harm, or damage.
<b>W</b>	
<b>Workplace Violence</b>	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.