INSIDER THREAT JOB AID

A Glossary of Basic Insider Threat Definitions

CDSE
Center For Development of Security Excellence

Basic Insider Threat Definitions

A

Access	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. National Industrial Security Program Operating Manual (NISPOM): The ability and opportunity to gain knowledge of classified information.
Adjudication	Evaluation of personnel security investigations and other relevant information to determine if it is clearly consistent with the interests of national security for persons to be granted or retain eligibility for access to classified information and continue to hold positions requiring a trustworthy decision.
Adverse Information	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.
Adversary	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.
Agent	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 (CI) purposes.
All-Source Analysis	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.
Analysis	The process by which information is transformed into intelligence; systemic examinations of information to identify significant facts, make judgments, and draw conclusions.

Basic Insider Threat Definitions

Anomalous Activity	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.
Asset	Person, structure, facility, information, material, or process that has value.

Basic Insider Threat Definitions

B

Background Investigation (BI)	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.
Behavioral Science	A branch of science (such as psychology, sociology, or anthropology) that primarily deals with human action and often seeks to generalize about human behavior in society.
Behavioral Science Consultant	A professional with extensive training in behavioral science, mental health, psychiatry, or psychology.

Basic Insider Threat Definitions

C

Chain of Custody	A chronological written record reflecting the release and receipt of evidence from initial acquisition until final disposition.
Civil Liberties	Rights granted to the people under the Constitution (and derived primarily from the First Amendment), to speak freely, think, assemble, organize, worship, or petition without government interference or restraints.
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 Information	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 Executive Order (EO) 13526, 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.
Clearance	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).
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.
Cleared Employee	All contractor employees granted personnel clearances and all employees being processed for clearances.

Basic Insider Threat Definitions

Cleared Defense Contractor (CDC)	A company or academic institution (i.e., university or college) that has entered into a security agreement with the Department of Defense (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.
Collection	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.
Company	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.
Compromised	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.
Cyber	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.
Cybersecurity	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.
Confidential	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.

Basic Insider Threat Definitions

Controlled Unclassified Information (CUI)	Unclassified information that does not meet the standards for National Security Classification under EO 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.
Counterintelligence (CI)	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.
Counterintelligence Inquiry	An examination of the facts surrounding an incident of potential CI interest, to determine if a CI investigation is necessary.
Counterintelligence Insider Threat (CI InT)	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).
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 Operations	Proactive activities designed to identify, deceive, exploit, disrupt, neutralize, or deter Foreign Intelligence Entity activities.
Countermeasure	Anything that effectively negates or mitigates an adversary's ability to exploit vulnerabilities.
Countermeasures	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.

Basic Insider Threat Definitions

Criminal Investigation	Investigation into alleged or apparent violations of law undertaken for purposes that include the collection of evidence in support of potential criminal prosecution.
Critical Asset	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.
Critical Infrastructure	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 deliberating impact on the security, national economic security, national public health and safety, or any combination of those matters.
Cyber Incident	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.
Cybersecurity	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. DoD Instruction (DoDI) 8500.01.
Cyber Threats	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.

Basic Insider Threat Definitions

D

Deception	An action intended by an actor to influence the perceptions, decisions, and actions of another.
Defense Security Counterintelligence Agency (DCSA)	An agency of the 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 DCSA. DCSA provides the military services, Defense Agencies, 24 federal agencies, and approximately 13,000 cleared contractor facilities with security support services.
Deterrence	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.
Disgruntled Employee	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.
Dissemination	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.
DoD Criminal Investigative Organizations	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.
DoD Insider Threat Management and Analysis Center (DITMAC)	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.

Basic Insider Threat Definitions

DoD Law Enforcement Agencies	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).
Due Process	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.

Basic Insider Threat Definitions

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.
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.
Espionage	Intelligence activity directed towards the acquisition of information through clandestine means.
Evidence	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.
Executive Order 12333 (EO 12333)	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, as amended.
Executive Order 13587 (EO 13587)	Executive order that directs United States Government executive branch departments and agencies (departments and agencies) to establish, implement, monitor, and report on the effectiveness of insider threat programs to protect classified national security information (as defined in Executive Order 13526; hereinafter classified information), and requires the development of an executive branch program for the deterrence, detection, and mitigation of insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. Full Title: Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.
Exploitation	The process of obtaining information from any source and taking advantage of it.

Basic Insider Threat Definitions

F

Federal Bureau of Investigation (FBI)	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.
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 (FISS) and international terrorist organizations.
Foreign Travel Brief	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.

Basic Insider Threat Definitions

H

Hacker	Unauthorized user who attempts to or gains access to an information system.
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	National standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA.
Honey Trap	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.
Human Resources	The personnel within the workforce including military officers and enlisted personnel (including members of the Reserve Components) and civilian employees working intelligence, counterintelligence, and security issues.

Basic Insider Threat Definitions

I

Inspector General (IG)	The criminal investigative arm of the Office of the Inspector General of the Department of Defense responsible for investigating: terrorism; technology/munitions theft & diversion; cybercrime; substandard/defective products; and fraud, bribery & corruption.
Illegal	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.
Indicator	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.
Industrial Security	That portion of information security that is concerned with the protection of classified information in the custody of U.S. industry.
Information Assurance (IA)	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.
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 EO, statute, or regulation. Information security includes protection of classified, controlled unclassified, and sensitive compartmented information.
Inquiry	The initial fact-finding and analysis process to determine the facts of any security incident.

Basic Insider Threat Definitions

Insider	DoD Directive (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. EO 13587: Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks or systems.
Insider Threat (InT)	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. EO 13587: The threat that an insider will use her/his 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.
Insider Threat Hub	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.
Intelligence Activities	All activities that elements of the Intelligence Community are authorized to conduct pursuant to EO 12333.

Basic Insider Threat Definitions

Intelligence Community (IC)	All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role.

Basic Insider Threat Definitions

K

Kinetic Violence	Deliberate application of force to the human body with the intent to do harm.

Basic Insider Threat Definitions

L

Law Enforcement	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.
Lawful Search	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.
Leaks	Deliberate disclosures of classified or unclassified information to the media.

Basic Insider Threat Definitions

M

Malicious Code	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.
Malware	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.
Mitigation	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.
Mole	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.

Basic Insider Threat Definitions

N

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 IAW EO 13587. The National Counter Intelligence Executive (NCIX) and FBI co-direct the daily activities of the NITTF.
Naval Criminal Investigative Service (NCIS)	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.
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. 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.
Network	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.

Basic Insider Threat Definitions

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.

Basic Insider Threat Definitions

P

Patterns	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.
Penetration	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.
Personally Identifiable Information (PII)	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.).
Personnel Security	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.
Physical Security	Security concerned with active, as well as passive measures, designed to deter intruders, prevent unauthorized access, including theft and damage, to assets such as personnel, equipment, installations, materials, and information, and to safeguard these assets against threats such as espionage, sabotage, terrorism, damage, and criminal activity.
Potential Risk Indicators	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.

Basic Insider Threat Definitions

Preliminary Inquiry	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.
Prevention, Assistance and Response (PAR)	A network of multi-disciplinary efforts, each led by a functional expert and normally resident on or available at the installation level, that commanders and their equivalent civilian leaders can use to aid them in identifying the level of risk that violent behavior poses to DoD personnel, organizations, installations, or separate facilities, and in developing risk-response recommendations to mitigate or remediate this risk.
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. 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.
Probable Cause	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.

Basic Insider Threat Definitions

R

Radicalization	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.
Records Check	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.
Recruitment	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.
Remediation	Actions taken to correct known deficiencies and weaknesses once vulnerability has been identified.
Reporting Requirements	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 Under Secretary of Defense for Intelligence and Security representatives, and will evolve over time.
Risk	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).
Risk Assessment	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.
Risk Management (RM)	The process of identifying, assessing, and controlling, risks arising from operational factors and making decisions that balance risk cost with mission benefits.

Basic Insider Threat Definitions

Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Basic Insider Threat Definitions

S

Sabotage	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.
Search	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.
Search Warrant	A document issued by a judicial officer that directs a LE 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.
Secret	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.
Section 811 Referral	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 (EB) agencies and departments and the FBI. Section 811 referrals are the reports – made by EB 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.
Security	Proactive measures adopted to safeguard personnel, information, operations, resources, technologies, facilities, and foreign relations against harm, loss, or hostile acts and influences.

Basic Insider Threat Definitions

Security Classification Guide (SCG)	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.
Security Clearance	An administrative determination by competent authority that an individual is eligible, from a security stand-point, for access to classified information.
Security Compromise	The disclosure of classified information to persons not authorized access thereto.
Security Countermeasures (SCM)	Actions, devices, procedures, and/or techniques to reduce security risks.
Security Incident	A security compromise, infraction, or violation.
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 Manager	A properly cleared individual having professional security credentials to serve as the manager for an activity.
Security Measures	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.
Seizure	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.
Senior official	The DoD official, designated by a DoD Component head, responsible for the direction, management, and oversight of the component's insider threat program.
Social Engineering	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.

Basic Insider Threat Definitions

Social Media	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.
Spills	Spills are the unintentional transfer of classified or proprietary information to unaccredited or unauthorized systems, individuals, applications, or media.
Subject	Person, place, or thing observed or is under investigation.
Suspect	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.

Basic Insider Threat Definitions

T

Threat	An adversary having the intent, capability, and opportunity to cause loss or damage.
Threat Analysis	A process that examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities.
Threat Assessment	A resultant product of the defined process used to conduct a threat analysis and develop an evaluation of a potential threat.
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.
Trade Secret Theft	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.

Basic Insider Threat Definitions

U

Unauthorized Disclosure	A communication or physical transfer of classified information to an unauthorized recipient.
User Activity Monitoring (UAM)	The technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing U.S. Government information in order to detect insider threat and to support authorized investigations.

Basic Insider Threat Definitions

V

Vulnerability	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.

Basic Insider Threat Definitions

W

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.