October
2024

A GLOSSARY OF BASIC INSIDER THREAT DEFINITIONS

JOB AID

CDSE Center for Development of Security Excellence

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

A

Access

The ability and opportunity to gain knowledge of classified information.

Adjudication

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

Adjudication and Vetting Services (AVS)

The sole authority to determine security clearance eligibility of non-Intelligence agency DOD personnel occupying sensitive positions or requiring access to classified material including Sensitive Compartmented Information (SCI).

Adversary

Any individual, group, organization, or government that conducts or has the intent and capability to conduct activities detrimental to the U.S. Government or its assets. Adversaries may include intelligence services, political or terrorist groups, criminals, and private interests.

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 may not be in the interest of national security, or that the individual is an insider threat.

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.

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

Air Force Office of Special Investigations (AFOSI)

The Department of the Air Force's major investigative service since Aug.1, 1948. The agency reports to the Inspector General, Office of the Secretary of the Air Force. AFOSI provides professional investigative service to commanders of all Department of the Air Force activities. Its primary responsibilities are criminal investigations and counterintelligence services.

Analysis

A detailed examination of anything complex in order to understand its nature or to determine its essential features: a thorough study.

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.

Army Counterintelligence (Army CI)

Conducts worldwide counterintelligence activities to detect, identify, neutralize, and exploit foreign intelligence entities, international terrorists, insider threats, and other foreign adversaries to protect the U.S. Army and DOD's strategic advantage.

Army Criminal Investigative Division (CID)

An independent federal law enforcement agency consisting of nearly 3,000 personnel assigned to 124 world-wide locations, responsible for felony criminal investigations and operations; war crimes and terrorism investigations, criminal intelligence collection and analysis; cybercrime investigations and operations; multi-dimensional forensic support; and protective service operations for the Secretary of Defense, Chairman of the Joint Chiefs of Staff, and other high-risk personnel.

Asset

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.

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 human behavior in society.

Behavioral Science Consultant

A professional with extensive training in behavioral science, mental health, psychiatry, or psychology.

C

Civil Liberties

Rights granted to the people under the Constitution (and derived primarily from the Bill of Rights), 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. Is the act or process by which information is determined to require protection against unauthorized disclosure and is marked to indicate its classified status.

Classified Information

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.

Clearance

Colloquial term for an eligibility determination made by an adjudicative office that an individual has authorized access, on a need-to-know basis, to a specific level of collateral classified information (TOP SECRET, SECRET, CONFIDENTIAL).

Cleared Contractor (CC)

A person or facility operating under the National Industrial Security Program (NISP) that has had an administrative determination that they are eligible for access to classified information of a certain level.

Cleared Employee

All contractor employees granted security clearances and all employees being processed for clearances.

Cleared Defense Contractor (CDC)

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.

Collection

The exploitation of sources by intelligence agencies, and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence.

Company

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 colloquial term referring to classified information received by a person not authorized to possess the information.

Concerning Behavior

Violations of policy and standard procedure, professional conduct, accepted practice, rules, regulations, or law through action or inaction (failure to report) that had been observed by managers, supervisors, and coworkers.

Confidential

Security classification that shall be applied to information, the unauthorized disclosure of which could reasonably be expected to cause damage to national security.

Continuous Evaluation (CE)

An Office of the Director of National Intelligence (ODNI) personnel security investigative process to review the background of a covered intelligence community individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. CE leverages a set of automated records checks and business rules to assist in the ongoing assessment of an individual's continued eligibility.

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

Continuous Vetting (CV)

A Defense Counterintelligence and Security Agency (DCSA) process that involves regularly reviewing a DOD-cleared individual's background to ensure they continue to meet security clearance requirements and should continue to hold positions of trust. Automated record checks pull data from criminal, terrorism, and financial databases, as well as public records, at any time during an individual's period of eligibility.

Controlled Unclassified Information (CUI)

Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information.

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

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 a Foreign Intelligence Entity (FIE).

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.

Countermeasure

Anything that effectively negates or mitigates an adversary's ability to exploit vulnerabilities.

Covered Person

A colloquial term referring to a person who is identified as being subject to a specific Systems of Records Notice.

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

Any process, program, or protocol 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.

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.

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 the cyberspace/cyber domain.

D

Data Spills

Data Spills occur when classified or controlled unclassified data is introduced either onto an unclassified information system or to an information system with a lower level of classification, or to a system not accredited to process data of that restrictive category.

Defense Security Counterintelligence Agency (DCSA)

An agency of the DOD with the mission of vetting, industry engagement, education, counterintelligence and insider threat support, secures the trustworthiness of the United States Government's workforce, the integrity of its cleared contractor support, and the uncompromised nature of its technologies, services, and supply chains.

Deterrence

The prevention from action by fear of the consequences. A state of mind brought about by the existence of a credible threat of unacceptable counteraction.

Devil's Advocacy

A Structured Analytic Technique that involves assuming a contrary or opposing viewpoint, often to test the strength of an argument, idea, or decision. It does not necessarily mean the advocate believes in the opposing viewpoint; rather, it is a way of encouraging critical thinking, exposing flaws in the original thinking, and preventing groupthink.

Disgruntled Employee

An employee who may be annoyed, discontent, displeased, dissatisfied, grumpy, irritated, malcontent, or upset to the point that he may take a malicious action against a coworker, supervisor, or employer.

Dissemination

The transmission, communication, sharing, or passing of information outside a Defense 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.

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

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 Inspector General for the DOD.

DOD Insider Threat Management and Analysis Center (DITMAC)

A component of the Defense Counterintelligence and Security Agency that provides the DOD enterprise a capability to identify, assess, and mitigate risk from insiders, to oversee and manage unauthorized disclosures, and to integrate, manage, mature, and professionalize insider threat (InT) capabilities.

DOD Law Enforcement Agencies

Organizations, agencies, entities, and offices of the Military Departments and Defense Agencies and the Inspector General of the DOD that perform an LE (law enforcement) function for those departments and agencies and are manned by DOD LEOs (Law Enforcement Officers).

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

The unauthorized disclosure of national defense information to a foreign power for the purpose of aiding the foreign power or injuring the United States.

Executive Order 12333 (EO 12333)

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)

Directs United States Government executive branch departments and agencies to establish, implement, monitor, and report on the effectiveness of insider threat programs to protect 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.

F

False Flag

A hostile or harmful action (such as an attack or intelligence activity) that is designed to look like it was perpetrated by someone other than the person or group responsible for it.

Federal Bureau of Investigation (FBI)

The primary investigative arm of the U.S. Department of Justice (DOJ) with jurisdiction over violations of more than 200 categories of federal law and a statutory member of the U.S. 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.

Fitness for Duty Evaluation (FFDE)

A required evaluation to determine whether an employee can meet the national security and/or professional requirements of a position with the Federal Government.

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 both foreign intelligence and security services (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.

H

Hacker

Colloquial term for an 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

Colloquial term for operations undertaken to ensnare an unwary target in a compromising sexual encounter that may leave the victim vulnerable to blackmail, which might result in the target committing espionage to avoid public disclosure.

Human Resources

A primary stakeholder within the counter insider threat domain that deals with the hiring, administration, training, and lifecycle of personnel. This stakeholder maintains employee performance records and is a valuable source of information for holistic behavioral data in the workplace. Additionally, this stakeholder is responsible for many mitigation actions.

I

Indicators or Signposts of Change

A type of Structured Analytic Technique (SAT) that uses historical data to expose trends and identify potential malicious acts. Two examples are counterintelligence indicators and potential risk indicators.

Inspector General (IG)

The IG promotes the economy, efficiency, and effectiveness of DOD programs, and the integrity of its workforce and operations, through impactful audits, evaluations, investigations, and reviews.

Illegal

Colloquial term for 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.

Industrial Security

The security discipline concerned with protection of classified U.S. Government and foreign government information, technologies, and material entrusted to cleared industry. DCSA administers the National Industrial Security Program (NISP) on behalf of the Department of Defense and 35 other federal agencies.

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.

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.

Insider

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

Insider Threat (InT)

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 composed of 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.

Intelligence Community (IC)

The U.S. IC includes 18 separate Government elements whose mission is to collect, analyze, and deliver foreign intelligence and counterintelligence information to America's leaders. Customers include the president, policymakers, law enforcement, and the military.

K

Kinetic Violence

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

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.

Leakage

A colloquial term referring to a type of warning behavior that typically infers a preoccupation with the target, and may signal the research, planning, and implementation of an attack.

Leaks

Colloquial term for an unauthorized disclosure to the media. Deliberate disclosures of classified or unclassified information to the media.

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 to annoy or disrupt the victim.

Military Criminal Investigative Organization (MCIO)

The Department of the Army Criminal Investigation Division, Naval Criminal Investigative Service, and Air Force Office of Special Investigations.

Military Department Counterintelligence Organization (MDCO)

The Department of the Army Counterintelligence Command, Naval Criminal Investigative Service, and Air Force Office of Special Investigations.

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 colloquial term for 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

National Insider Threat Task Force (NITTF)

A task force with the mission to develop a Government-wide insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies.

National Security Eligibility Determination

A determination that a person is able and willing to safeguard classified national security information and/or occupy a national security sensitive position. The three national security clearance eligibility levels are: Confidential, Secret, and Top Secret.

Naval Criminal Investigative Service (NCIS)

The federal law enforcement agency/counterintelligence organization 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 warnings and specialized defensive force protection support to U.S. naval forces around the world.

Need-to-know

A determination made by an authorized holder of classified information or controlled unclassified information (CUI) that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified information/CUI to perform tasks or services.

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.

O

Open Source

Information derived exclusively from publicly or commercially available sources.

P

Personally Identifiable Information (PII)

Any information that can be used to distinguish or trace a person's identity. Examples of personally identifiable information (PII) include: Social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, financial account, credit card number, personal address, and personal phone number.

Personal Predispositions

The personal characteristics that predispose individuals toward becoming insider risks; potential foundations for insider risk such as biased judgment, a propensity for rule violation, and the potential for the creation of adversarial identification or affiliation.

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

The security discipline that is 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.

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. Commanders and their equivalent civilian leaders can use it to identify 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. 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.

Problematic Organizational Response

An organization's response to the concerning behaviors of at-risk employees, including inaction, inattentiveness, or lack of understanding of their risk factors.

Protected Health Information (PHI)

Any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.

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 extremism, but involvement in extremism 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.

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 a vulnerability has been identified.

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.

Risk Mitigation

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

Routine Use Disclosure Exception

Allows disclosures of information outside of an agency without the request of consent of the person the record pertains to when the disclosure is compatible with the purpose for which the record was collected.

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 or by consent, 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 an 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.

Security Classification Guide (SCG)

A documentary form of classification guidance issued by an original classification authority (OCA) that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

Security Clearance

An administrative determination by a competent authority that an individual is eligible, from a security standpoint, for access to classified information.

Security Compromise

The disclosure of classified or controlled unclassified information to persons not authorized to access it.

Security Countermeasures (SCM)

Actions, devices, procedures, and/or techniques to reduce security risks.

Security Incident

A security compromise, infraction, or violation.

Security Infraction

Any knowing, willful, or negligent action contrary to the requirements of Executive Order 13526, "Classified National Security Information," December 29, 2009, its implementing directives, that does not constitute a "security violation,"

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.

Security Violation

Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information.

Senior Official

A person designated by an agency head to be principally responsible for establishing a process to gather, integrate, centrally analyze, and respond to Counterintelligence (CI), Security, Information Assurance (IA), Human Resources (HR), Law Enforcement (LE), and other relevant information indicative of a potential insider threat.

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.

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.

Stressors

Events (both positive and negative) that result in changes in personal, social, or professional responsibilities that require people to spend effort and energy to adjust.

Structured Analytic Technique (SAT)

A "box of tools" to help the analyst mitigate the adverse impact on analysis of one's cognitive limitations and pitfalls.

Structured Professional Judgement (SPJ)

An evidence-based approach to effectively assess and manage the associated risks from a potential workplace violence risk that combines empirically validated tools with professional judgment.

System of Records Notice (SORN)

Informs the public of the purpose of the system, authority for maintaining the system, and the type of records the system contains. It also provides instructions on how the information in the system can be routinely used and additional details about the system.

Subject

Person, place, or entity 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.

T

Threat

A person or entity having the intent, capability, and opportunity to cause loss or damage.

Threat Assessment

The practice of determining the credibility and seriousness of a potential threat, as well as the probability that the threat will become a reality.

Top Secret

Security classification that shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

Trade Secret

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

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.

Trusted Workforce 2.0

A whole-of-Government background investigation reform effort that is overhauling the personnel vetting process by establishing a Government-wide system enhancing security, allowing reciprocity across organizations, and generating cost savings across Government. This includes replacing periodic reinvestigations with a continuous vetting (CV) program, ensuring a trusted workforce in near real time through automated records checks and inter-agency information sharing.

U

Unauthorized Disclosure

A communication or physical transfer of classified information or unclassified controlled 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 to detect insider threats and to support authorized investigations.

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.

W

Within Agency "need to know" Disclosure Exception

Authorizes the intra-agency disclosure without the request of consent of the person the record pertains to for necessary, official purposes.

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.