Glossary

Course: Establishing an Insider Threat Program for Your Organization

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

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

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

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

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

Compromise: An unauthorized disclosure of classified information.

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

Counterintelligence: Information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities. (EO 12333, as amended)

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

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

Espionage: Defined under Sections 792-799, Chapter 37, title 18, United States Code (reference: Sections 792-799, Chapter 37 of title 18, United States Code) and Article 106a, Uniform Code of Military Justice (UCMJ) (reference: Section 801-940, Chapter 47, of title 10, United States Code, Uniform Code of Military Justice). Espionage is the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. The offense of espionage applies during war or peace. Reference (Sections 792-799, Chapter 37 of title 18, United States Code) makes it an offense to gather, with the requisite intent or belief, national defense information, by going on, entering, flying over, or obtaining access by any means to any installation or place used by the United States for national defense. The method of gathering that information is immaterial. Anyone who lawfully or unlawfully is entrusted with or otherwise has possession of, access to, or control over information about national defense, which he or she has reason to believe could be used against the United States or to the advantage of any foreign nation, and willfully communicates or transmits, or attempts to communicate or transmit, such information to any person not entitled to receive it may be punished under reference (Sections 792-799, Chapter 37 of title 18, United States Code). Anyone entrusted with or having lawful possession or control of information about national defense, who through gross negligence permits the same to be lost, stolen, abstracted, destroyed, removed from its proper place of custody, or delivered to anyone in violation of that trust may be punished under reference (Sections 792-799, Chapter 37 of title 18, United States Code). If two or more persons conspire to commit and one of them commits an overt act in furtherance of such conspiracy, all members of the conspiracy may be punished for violation of reference (Sections 792-799, Chapter 37 of title 18, United States Code).

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

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

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

Sabotage: An act or acts with the intent to injure or interfere with, or obstruct the national defense of a country by willfully injuring, destroying, or attempting to destroy any national defense or war materiel, premises or utilities to include human or natural resources, under reference (Sections 792-799, Chapter 37 of title 18, United States Code).

Security: A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

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

Terrorism: The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Treason: Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason (see Section 2831 of title 18, U.S. Code, reference (Sections 792-799, Chapter 37 of title 18, United States Code).

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

Unwitting: Inadvertent or accidental