Glossary

Course: Storage Containers and Facilities

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

Activity Security Manager: Individual specifically designated in writing and responsible for an activity's information security program who ensures classified and controlled unclassified information is properly handled during its entire life cycle. That overview includes ensuring material is appropriately identified, marked, stored, disseminated, disposed of, and accounted for, as well as providing guidance on the handling of security incidents to minimize adverse effects and ensure that appropriate corrective action is taken. The security manager may be assigned responsibilities in other security disciplines such as personnel and physical security.

Agency: An organization specified as such in E.O. 12958 (reference (e)), as amended by E.O. 12972 (reference (f)). Within the Department of Defense, this term includes the Department of Defense and the Departments of the Army, the Navy, and the Air Force.

Applicable Associated Markings: Markings, other than those that designate classification level, that are required to be placed on classified documents. These include the "classified by" line, downgrading and declassification instructions, special control notices, Special Access Program caveats, etc.

Approved Access Control Device: Any access control device that meets the requirements of Department of Defense 5220.22-M as approved by the Facility Security Officer.

Approved Built-in Combination Lock: Combination lock, equipped with a top reading dial conforming to Underwriters Laboratory Standard Number UL 768, Group IR

Approved Combination Padlock: Three-position, dial-type changeable combination padlock listed on the Government Services Administration Qualified Products List as meeting the requirements of Federal Specification FF-P-110.

Approved Electronic, Mechanical, or Electro-Mechanical Device: Specific device meeting the requirements of Department of Defense standard 5220.22-M as approved by the Facility Security Officer.

Approved Key-Operated Padlock: Padlock meeting the requirements of MIL-SPEC-P-43607 (shrouded shackle), National Stock Number 5340-00-799-8248, or MIL-SPEC-P-43951 (regular shackle), National Stock Number 5340-00-799-8016

Approved Security Container: Security file container, originally procured from a Federal Supply Schedule supplier, conforming to Federal specifications and bears a "Test Certification Label" on the locking drawer attesting to the security capabilities of the container and lock. Such containers must be labeled "General Services Administration Approved Security Container" on the face of the top drawer. Acceptable tests of the containers can be performed only by a testing facility specifically approved by General Services Administration.

Approved Vault: Vault constructed in accordance with Department of Defense Standard 5220.22-M and approved by the General Services Administration.

Area Security: Consolidating assets into one area, installation, or facility and increasing the security for that particular area

Ammunition: A device charged with explosives, propellants, pyrotechnics, initiating composition, riot control agents, chemical herbicides, smoke and flame, for use in connection with defense or offense, including demolition. Excluded from this definition are devices charged with chemical agents defined in Joint Chiefs of Staff Pub. 1 and nuclear or biological materiel. Ammunition includes cartridges, projectiles, including missile rounds, grenades, mines, and pyrotechnics together with bullets, shot and their necessary primers, propellants, fuses, and detonators individually or having a unit of issue, container, or package weight of 100 pounds or less. Blank, inert training ammunition and caliber .22 ammunition are excluded.

Arms: A weapon included in AR 190–11, appendix A, that will or is designated to expel a projectile or flame by the action of the explosive, and the frame or receiver of any such weapon.

Asset: Resource—person, group, relationship, instrument installation, supply—at the disposition of an intelligence agency for use in an operational or support role. A person who contributes to a clandestine mission but is not a fully controlled agent

Automated Information System (AIS): An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

Capability: Facilitating method to implement a course of action. (A capability may or may not be accompanied by an intention)

CCTV: Closed circuit television is a security system with a camera that captures an image, converts it to a video signal, and transmits it to a monitoring station.

Classified National Security Information (Or "Classified Information"): Information that has been determined pursuant to E.O. 12958 (reference (e)) or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Cognizant Security Agent: Security cognizance remains with each Federal department or agency unless lawfully delegated. The term Cognizant Security Agency denotes the Department of Defense, Department of Energy, Nuclear Regulatory Commission, and Central Intelligence Agency. The Secretary of Defense, the Secretary of Energy, the Director of the Central Intelligence Agency and the Chairman, Nuclear Regulatory Commission may delegate any aspect of security administration regarding classified activities and contracts under their purview within the Cognizant Security Agency or to another Cognizant Security Agency. Responsibility for security administration may be further delegated by a Cognizant Security Agency to one or more Cognizant Security Offices. It is the obligation of each Cognizant Security Agency to inform industry of the applicable Cognizant Security Offices.

Collateral Information: Information identified as National Security Information under the provisions of E.O. 12958 (reference (e)) but that is not subject to enhanced security protection required for SAP Information.

Communications Security (COMSEC): The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes crypto-security, emission security, transmission security, and physical security of COMSEC material and information.

Compromise: An unauthorized disclosure of classified information.

Counterintelligence: The act of keeping sensitive information from an enemy, deceiving that enemy, preventing subversion and sabotage, and collecting political and military information.

Covert Entry: Operation that is so planned and executed as to conceal the identity of, or permit plausible denial by, the sponsor. A covert operation differs from a clandestine operation in that emphasis is placed on concealment of the identity of the sponsor rather than on concealment of the operation.

Damage to National Security: Harm to the national defense or foreign relations of the United States from unauthorized disclosure of information, including the sensitivity, value, and utility of that information

Deadly Force: Force that a person uses causing, or that a person knows or should know would create a substantial risk of causing, death or serious bodily harm.

Director of Central Intelligence Directive: Directive issued by the Director of Central Intelligence that establishes general policies and procedures to be followed by intelligence agencies and organizations under his jurisdiction before passage of the Intelligence Reform and Terrorism Prevention Act. Future Intelligence Community Directives, Intelligence Community Policy Guidance documents issued by the Director of National Intelligence will supersede Director of Central Intelligence Directives.

Document: Any physical medium in or on which information is recorded or stored, to include written or printed matter, audiovisual materials, and electromagnetic storage media.

DoD Components: The Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, and the Defense Agencies.

Electronic Security Systems (ESS): That part of physical security concerned with the safeguarding of personnel and property by use of electronic systems. These systems include, but are not limited to, intrusion detection systems (IDS), automated entry control systems (AECS), and video assessment systems.

Explosives: Any chemical compound, mixture or device, the primary or common purpose of which is to function by explosion. The term includes, but is not limited to, individual land mines, demolition charges, blocks of explosives (dynamite, Trinitrotoluene, C–4, and other high explosives), and other explosives consisting of 10 pounds or more; for example, gunpowder or nitroguanidine.

Facility: Buildings, structures, or other real property. Entities such as military bases, industrial sites, and office complexes may be identified as facilities. Plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operational entity.

Forced Entry: Entry by an unauthorized individual who leaves evidence of the act

Foreign Government Information: Information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; Information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or Information received and treated as "Foreign Government Information" under the terms of a predecessor order to E.O. 12958 (reference (e)).

General Services Administration: Independent agency of the U.S. Government, established in 1949 to help manage and support the basic functioning of Federal agencies. The General Services Administration supplies products and communications for U.S. Government offices, provides transportation and office space to Federal employees, and develops Government wide, cost-minimizing policies, among other management tasks. Its stated mission is to “help Federal agencies better serve the public by offering, at best value, superior workplaces, expert solutions, acquisition services and management policies.”

Government-Approved Facility: Government-owned room or outside of a Special Access Program Facility with controlled or restricted assess designed to limit public access that has operational procedures in place to actually limit access; any Government-owned Special Access Program Facility or area within a Special Access Program Facility.

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the Agency that originates information, or its successor in function, to regulate access to the information.

Information Security: The system of policies, procedures, and requirements established under the authority of E.O. 12958 (reference (e)) to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

Installations: Real DoD properties including bases, stations, forts (including National Guard and Federal Reserve Centers), depots, arsenals, plants (both contractor and Government operated), hospitals, terminals, and other special mission facilities, as well as those used primarily for military purposes.

Integrity: The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

Intelligence Activity: An activity that an Agency within the Intelligence Community is authorized to conduct under E.O. 12333 (reference (c)).

Intrusion Detection System: A security system that is designed to detect a change in the environment and transmit some type of alarm notification.

Material: Any product or substance on or in which information is embodied.

National Security: The national defense or foreign relations of the United States.

Need-To-Know: A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Physical Security: The security discipline concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

Protective Security Service: A transportation protective Service provided by a cleared commercial carrier qualified by the Military Traffic Management Command (MTMC) to transport SECRET shipments. The carrier must provide continuous attendance and surveillance of the shipment by qualified carrier representatives and maintain a signature and tally record. In the case of air movement, however, observation of the shipment is not required during the period it is stored in the carrier's aircraft in connection with flight, provided the shipment is loaded into a compartment that is not accessible to an unauthorized person aboard. Conversely, if the shipment is loaded into a compartment of the aircraft that is accessible to an unauthorized person

aboard, the shipment must remain under the constant surveillance of a cleared escort or qualified carrier representative.

Restricted Area: An area (land, sea or air) in which there are special restrictive measures employed to prevent or minimize incursions and/or interference, where special security measures are employed to prevent unauthorized entry. Restricted areas may be of different types depending on the nature and varying degree of importance of the security interest, or other matter contained therein. Restricted areas must be authorized by the installation/activity commander/director, properly posted, and shall employ physical security measures. Additionally, Controlled Areas may be established adjacent to Restricted Areas for verification and authentication of personnel.

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).

Sabotage: Destruction of an employer's property (as tools or materials) or the hindering of manufacturing by discontented workers; destructive or obstructive action carried on by a civilian or enemy agent to hinder a nation's war effort; an act or process tending to hamper or hurt.

Safeguarding: Measures and controls that are prescribed to protect classified information

Secure Working Area: Accredited facility or area that is used for handling, discussing and/or processing, but not storage of Special Access Program information.

Security Clearance: A determination that a person is eligible under the standards of DoD 5200.2-R (reference (ss)) for access to classified information.

Security-in-Depth: A determination by the senior agency official that a facility's security program consists of layered and complimentary security controls sufficient to deter, detect, and document unauthorized entry and movement within the facility. Examples include the use of perimeter fences, employee and visitor access controls, use of an intrusion detection system, random guard patrols throughout the facility during nonworking and working hours, and closed circuit video monitoring or other safeguards that mitigate the vulnerability of unalarmed storage areas and security storage cabinets during non-working hours.

Senior Agency Official: An official appointed by the Secretary of Defense, Secretary of the Army, Secretary of the Navy, or Secretary of the Air Force under the provisions of Section 5.6(c) of E.O. 12958 (reference (e)).

Senior Official: An official appointed by the Head of a DoD Component to be responsible for direction and administration of the Information Security Program. (NOTE: In the Departments of Defense, Army, Navy, and Air Force, this official will also be the "Senior Agency Official," as defined above.)

Sensitive Compartmented Information (SCI): Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the Director of Central Intelligence.

Sensitive Compartmented Information Facility (SCIF): Sensitive Compartmented Information Facility is an area, room (or set of rooms), building installation accredited to store, use, discuss, or electronically process Sensitive Compartmented Information. The standards and procedures for a Sensitive Compartmented Information Facility are stated in Director of Central Intelligence Directives 1/19 and 1/21.

Sensitive Items: Material requiring a high degree of protection to prevent unauthorized acquisition. This includes arms, ammunition, explosives, drugs, precious metals, or other

substances determined by the Administrator, Drug Enforcement Administration to be designated Schedule Symbol II, III, IV, or V under the Controlled Substance Act of 1970.

Surreptitious Entry: Unauthorized entry in a manner that leaves no readily discernible evidence.

Theft: The unlawful taking and removing of property with intent to deprive the rightful owner of it.

Threat: The perceived imminence of intended aggression by a capable entity to harm a nation, a government or its instrumentalities, such as intelligence, programs, operations, people, installations, or facilities.

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

Violation: Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of E.O. 12958 (reference (e)) or its implementing directives; Any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of reference (e).

Vulnerability: A situation or circumstance, which left unchanged, may result in the degradation, loss of life, or damage to mission-essential resources.