Glossary

Course: Cybersecurity Awareness

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

Access Control: The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).

Anomalies: Foreign power activity or knowledge suggesting foreign knowledge of U.S. national security information, processes or capabilities.

Application: Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.

Asset: A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Assurance: Measure of confidence that the security features, practices, procedures and architecture of an IT system accurately mediates and enforces the security policy.

Audit: Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures.

Authentication: The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authority: Person(s) or established bodies with rights and responsibilities to exert control in an administrative sphere.

Authorization: Access privileges granted to a user, program, or process or the act of granting those privileges.

Authorized Person: A person who has a need-to-know for classified information in the performance of official duties and who has been granted a PCL at the required level

Availability: The property of being accessible and useable upon demand by an authorized entity. Ensuring timely and reliable access to and use of information.

Baseline: Hardware, software, databases, and relevant documentation for an information system at a given point in time.

Boundary: Physical or logical perimeter of a system.

Certificate: A digitally signed representation of information that:

1) Identifies the authority issuing it,
2) Identifies the subscriber,
3) Identifies its valid operational period (date issued / expiration date).

In the IA community "certificate" usually implies public key certificate and can have the following types:

Cross certificate: A certificate issued from a certification authority (CA) that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two CAs.

Encryption certificate: A certificate containing a public key that can encrypt or decrypt electronic messages, files, documents, or data transmissions, or establish or exchange a session key for these same purposes. Key management sometimes refers to the process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate.

Classified Information: See classified national security information.

Classified Information Spillage (aka Spill): Security incident that occurs whenever classified data is spilled either onto an unclassified information system or to an information system with a lower level of classification.

Classified National Security Information (CNSI): Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure in the interest of national security and is marked to indicate its classified status when in documentary form

Clearance: Formal certification of authorization to have access to classified information other than that protected in a special access program (including SCI). Clearances are of three types: confidential, secret, and top secret. A top secret clearance permits access to top secret, secret, and confidential material; a secret clearance, to secret and confidential material; and a confidential clearance, to confidential material.

Clearing: Removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., through the keyboard); however, the data may be reconstructed using laboratory methods.

Cleared Contractor (CC): A person or facility operating under the NISP, which 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). There are approximately 8500 cleared contractors with over 13,000 facilities.

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.

Cloud Computing: A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), and Cloud Infrastructure as a Service (IaaS)); and four models for enterprise access (Private cloud, Community cloud, Public cloud and Hybrid cloud).
Note: Both the user's data and essential security services may reside in and be managed within the network cloud.

Collateral: All national security information classified Confidential, Secret, or Top Secret under the provisions of an Executive order for which special systems of compartmentation (such as SCI or SAPs) are not formally required.

Common Access Card (CAC): Standard identification/smart card issued by the Department of Defense that has an embedded integrated chip storing public key infrastructure (PKI) certificates.

Communications Security (COMSEC): A component of cybersecurity that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material.

Controlled Unclassified Information (CUI): A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Section 403 of title 50, United States Code “National Security Act of 1947”, but is pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. The designation CUI includes the term “sensitive but unclassified” (SBU).

Command Cyber Readiness Inspection (CCRI): The purpose of the CCRI is to improve the overall security posture of the Global Information Grid (GIG) through a formal inspection process, and hold the commanders and directors of COCOMs, Services and Agencies on both NIPRNet and SIPRNet accountable for their respective security posture. The CCRI grades and measures security posture via a review of technology areas, vulnerability scan results, compliance with issued directives, and non-technical aspects of the site’s cybersecurity.

Company: A generic and comprehensive term which may include sole proprietorships, individuals, partnerships, corporations, societies, associations, and organizations usually established and operating to commonly prosecute a commercial, industrial or other legitimate business, enterprise, or undertaking.

Comprehensive National Cybersecurity Initiative (CNCI) (NSPD-54/ HSPD-23): Authorizes DHS, together with OMB, to establish minimum operational standards for Federal Executive Branch civilian networks so that US-CERT can direct the operation and defense of government connections to the Internet. Empowers DHS to lead and coordinate the national effort in the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure availability, integrity, authenticity, confidentiality, and non-repudiation is maintained across cyberspace.

Compromise: An unauthorized disclosure of classified information.

Computer Network Attack (CNA): Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Computer Network Defense (CND): Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.

Computer Network Exploitation (CNE): Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks.

Computer Network Operations (CNO): Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.

Computer Network Defense Service Provider (CNDSP): Those organizations responsible for delivering computer network defense services to owners of DoD information systems. There are three primary CND Services; Protect; Monitor, Analyze and Detect; and Respond. These services include actions employed to prevent or lessen computer network attacks that may disrupt, deny, degrade, destroy, exploit, allow unauthorized access to, or facilitate information theft from computer networks, ISs, or their contents.

Confidential: The classification level applied to information, the unauthorized disclosure of which reasonable could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

Confidentiality: The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary 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.

Control: The authority of the agency that originates information, or its successor in function, to regulate access to the information.

Continuous Monitoring: The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: 1) The development of a strategy to regularly evaluate selected IA controls/metrics, 2) Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events, 3) Recording changes to IA controls, or changes that affect IA risks, and 4) Publishing the current security status to enable information sharing decisions involving the enterprise.

Counterintelligence: 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. (EO 12333, amended 30 July 2008)

Counterintelligence Investigations: Are conducted to prove or disprove an allegation of espionage or other intelligence activities, such as sabotage, assassination, or other national security crimes conducted by or on behalf of a foreign government, organization, or person or international terrorists. CI investigations may establish the elements of proof for prosecution or administrative actions, provide a basis for CI operations, or validate the suitability of personnel for access to classified information. CI investigations are conducted against individuals or groups for committing major security violations, as well as failure to follow Defense Agency and Military Department directives governing reporting contacts with foreign citizens and out-of-channel requests for defense information. CI investigations provide military commanders and policymakers with information used to eliminate security vulnerabilities and otherwise improve the security posture of threatened interests.

Cyber Attack: An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Espionage: The act of obtaining sensitive, proprietary or classified information from individuals, competitors, groups, or governments for military, political, or economic advantage using various computer exploitation methods often facilitated through cyber incidents.

Cyber Incident: Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. Synonymous with the term "Cyber Event."

CYBERCOM: An Armed Forces sub-unified command subordinate to United States Strategic Command. CYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.

Cybersecurity: Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Cyberspace: A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Data Asset: 1. Any entity that is comprised of data. For example, a database is a data asset that is comprised of data records. A data asset may be a system or application output file, database, document, or web page. A data asset also includes a service that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a web site that returns data in response to specific queries (e.g., www.weather.com) would be a data asset. 2. An information-based resource.

Defense Cyber Crime Center (DC3): One of the designated national cyber centers established in accordance with NSPD54/HSPD23, per DoDD 5505.13E. Among its tasks, DC3 is to:

- Serve as one of the designated national cyber centers in accordance with NSPD 54 & HSPD 23
- Serve as operational focal point for DIB CS / IA information sharing and digital forensics analysis activities performed to protect DoD unclassified info on unclassified DIB information systems
- Support DoD critical infrastructure protection by enhancing the cybersecurity of the DIB against cyber threats and crimes
- Serve as the DoD Center of Excellence and establish DoD standards for digital and multimedia forensics
- Develop and provide specialized cyber investigative training for DoD & non-DoD personnel, as authorized
- Maintain a central clearinghouse and repository for cyber CI tools, techniques, or other procedures and share them with other DoD CI components

Defense-in-Depth: Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

Defense Industrial Base (DIB): The Department of Defense (DoD), government, and private sector worldwide industrial complex with the capabilities of performing research and development, design, production, delivery, and maintenance of military weapons systems, subsystems, components, or parts to meet military requirements. The DIB includes tens of thousands of companies and their subcontractors who perform under contract to DoD, and companies providing incidental materials and services to DoD, as well as government-owned/contractor-operated and government-owned/government-operated facilities. DIB companies include domestic and foreign entities, with production assets located in many countries. The DIB includes companies performing on contracts of all classification levels; therefore, it is *not* limited to those cleared contractors under the NISP which have defense contracts. It is estimated there are 65,000+ defense contractors within the DIB, the great majority of which are not cleared under the NISP.

Because only a small fraction of DIB facilities are DoD-owned, DoD and government actions focus to support private owner/operator efforts at DIB facilities determined to be critical to national security.

DIB Cyber Security/Information Assurance Program (DIB CS/IA): A program created by DoDI 5205.13 for the increasing DoD support for cleared contractors' efforts to protect unclassified DoD information that transits / resides on cleared contractor unclassified IT systems. Therefore, a DoD-DIB partnership was created that facilitates DoD coordination of unclassified and classified cyber threat information with the DIB, standard procedures for DIB incident reporting and response, and standard procedures for cyber-intrusion damage assessment and remediation support to the DIB.

Document: Any recorded information, regardless of its physical form or characteristics, including, without limitation, written or printed matter, tapes, charts, maps, paintings, drawing, engravings, sketches, working notes and papers; reproductions of such things by any means or process; and sound, voice, magnetic, or electronic recordings in any form.

DoD Component CI Organizations: The organic CI elements of the Army, the Navy, the Air Force, the Marine Corps, the Joint Staff, the Combatant Command Staffs, the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the Defense Security Service, the Defense Threat Reduction Agency, and the Missile Defense Agency and the CIFA.

Domain: An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See also security domain.

Electronic Credentials: Digital documents used in authentication that bind an identity or an attribute to a subscriber's token.

Electronic Signature: The process of applying any mark in electronic form with the intent to sign a data object. See also digital signature.

Enclave: Collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

Enclave boundary: Point at which an enclave's internal network service layer connects to an external network's service layer, i.e., to another enclave or to a Wide Area Network (WAN).

Embedded System: An IS that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem such as, ground support equipment, flight simulators, engine test stands, or fire control systems.

Environment: Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an IT system.

Espionage: 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. Espionage is a national security crime under Title 18 USC, §§ 792-798 and Article 106, Uniform Code of Military Justice (UCMJ) and carries punishments up to and including fine, imprisonment, and death.

Encryption: The process of changing plaintext into cipher text for the purpose of security or privacy.

Enterprise: An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management.

Event: Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.

Exfiltration: The unauthorized removal of data or files from a system by an intruder

Facility: A 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 operating entity. (A business or educational organization may consist of one or more facilities as defined herein.) For purposes of industrial security, the term does not include Government installations.

Facility (Security) Clearance (FCL): An administrative determination that, from a security viewpoint, a company is eligible for access to classified information of a certain category (and all lower categories).

Federal Information System: An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

Firewall: A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy.

Firmware: Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.

Foreign Diplomatic Establishment: Any embassy, consulate, or interest section representing a foreign country.

Foreign Government Information (FGI): Information that is: a. Provided to the U.S. by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or b: Produced by the U.S. pursuant to, or as a result of, a joint arrangement with a foreign government or

governments, an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence.

Government Contracting Activity (GCA): An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.

Industrial Security: That portion of information security which is concerned with the protection of classified information in the custody of U.S. industry.

Information: Any knowledge that may be communicated or documentary material, regardless of its physical form or characteristics.

Information Security (INFOSEC): Protection of ISs against unauthorized access to information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter threats.

Information System (IS) (aka System): Any telecommunication or computer-related equipment or interconnected system or sub-systems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of voice or data, and includes software, firmware and hardware. An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information and textual material.

Lead CI Agency: A Military Department CI Agency that has been designated by the USD(I) to provide defined levels of CI support to one or more of the DoD Components.

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

Military Department CI Agencies: The Military Department CI Agencies include the U.S. Army Counterintelligence, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations.

National Industrial Security Program (NISP): The National Industrial Security Program (NISP) is a partnership between the federal government and private industry to safeguard classified information. Executive Order 12829, as amended, National Industrial Security Program was established to achieve cost savings and protect classified information held by contractors, licensees, and grantees of the United States Government. The Order was signed by President Bush in January of 1993. The NISP affects all executive branch agencies. The major signatories to the program are the Department of Energy, the Nuclear Regulatory Commission, the Department of Defense, and the Central Intelligence Agency (CSAs). DoD is the Executive Agent for DoD and 23 other federal agencies.

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

National Security System (NSS): Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an

agency, or other organization on behalf of an agency whereas the function, operation, or use of which:

(I) involves intelligence activities;
(II) involves cryptologic activities related to national security;
(III) involves command and control of military forces;
(IV) involves equipment that is an integral part of a weapon or weapons system; or
(V) is critical to the direct fulfillment of military or intelligence missions; or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Guard (system): A mechanism limiting the exchange of information between information systems or sub-systems.

Hacker: Unauthorized user who attempts to or gains access to an information system.

High-Impact System: An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of high.

Identity Certificate: A certificate that provides authentication of the identity claimed. Within the NSS PKI, identity certificates may be used only for authentication or may be used for both authentication and digital signatures.

Incident: An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Indicator: Recognized action, specific, generalized, or theoretical, that an adversary might be expected to take in preparation for an attack.

Information: Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Information Assurance: See Cybersecurity.

Information System (IS) (aka System): A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

Information Technology (IT): Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive

agency which 1) requires the use of such equipment or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Integrity: The property whereby an entity has not been modified in an unauthorized manner. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Internet: The Internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the IAB and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

Intranet: A private network that is employed within the confines of a given enterprise (e.g., internal to a business or agency).

Intrusion: Unauthorized act of bypassing the security mechanisms of a system.

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. Spyware and some forms of adware are also examples of malicious code.

Malicious Logic: Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.

Malware: See malicious code, malicious applets, and malicious logic.

Media: Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Media Sanitization: The actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

Need-to-Know: A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official United States Government program. Knowledge, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

Network: A system of two or more IS that can exchange data or information.

Object: Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object implies access to the information it contains.

Penetration Testing: A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.

Portable Electronic Device (PED): Any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, video cameras, and pagers.

Prevalence: The number of enclaves affected by a cyber incident.

Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Records: The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

Remote Terminal: A device for communication with an automated information system from a location that is not within the central computer facility.

Robustness: The ability of a cybersecurity entity to operate correctly and reliably across a wide range of operational conditions, and to fail gracefully outside of that operational range.

Role: A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks.

Root level intrusion: Provides the intruder unrestricted system access, to include administrator privileges

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).

Sanitization: A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.

SCI: SCI is classified intelligence information concerning or derived from sensitive sources, methods, or analytical processes, which is required to be handled exclusively within formal access control systems established by the DNI.

SECRET: The classification level 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.

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.

Sensitive Information: Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L.100-235).) See also controlled unclassified information (CUI).

Sensitivity: A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

Social Engineering: An attempt to trick someone into revealing information (e.g., a password) that can be used to attack an enterprise.

Social Networking: The use of collaborative sites, mostly Internet-based, to post and combine digital content, such as text, video, audio, and geographic from multiple sources, usually to enhance the online description of an idea or concept, facilitate interpersonal relationships between familiar or unfamiliar users, and/or convey messages to targeted audiences.

Software: Computer programs and associated data that may be dynamically written or modified during execution.

Spying: See Espionage.

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.

System: Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. See also information system.

System Software: Computer programs that control, monitor, or facilitate use of the IS; for example, operating systems, programming languages, communication, input/output control, sorts, security packages and other utility type programs. Considered to also include off-the-shelf application packages obtained from manufacturers and commercial

vendors, such as for word processing, spreadsheets, data base management, graphics, and computer-aided design.

Technical Data: Information governed by Title 22, Code of Federal Regulations, Parts 120-130, "International Traffic in Arms Regulations" (ITAR) and the Export Administration Regulation (EAR). The export of technical data that is inherently military in character is controlled by Title15, Code of Federal Regulations, parts 368.1-399.2, "Export Administration Regulation (EAR)" The export of technical

Technical Security Controls: Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Technical Vulnerability Information: Detailed description of a weakness to include the implementable steps (such as code) necessary to exploit that weakness.

Telecommunications: Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

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.

TOP SECRET: The classification level applied to information, the unauthorized disclosure of which reasonable could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

Transmission: The sending of information from one place to another by radio, microwave, laser, or other non-connective methods, as well as by cable, wire, or other connective medium. Transmission also includes movement involving the actual transfer of custody and responsibility for a document or other classified material from one authorized addressee to another.

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 Person: A person not authorized to have access to specific classified information in accordance with the requirements of the NISPOM.

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

United States Computer Emergency Readiness Team (US-CERT): US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local government, industry and international partners. US-CERT interacts with

federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cybersecurity information to the public.

Unauthorized Access: Any access that violates the stated security policy.

Unauthorized Disclosure: An event involving the exposure of information to entities not authorized access to the information.

User: Individual, or (system) process acting on behalf of an individual, authorized to access an information system. Person or process authorized to access an IT system.

User Code: Software that allows a user to modify data or functions of an IS. Determining if an IS has user code may be a matter of degree, but as an example, if an IS only has a button that performs a single function when pressed, the IS is considered to have no user code on it. If the user can input classified information and save it to the IS then the IS certainly has user code.

User level intrusion: Provides the intruder restricted system access based on privileges granted to the user

Validation: Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes or requirements).

Virus: A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Worm: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Wide Area Network (WAN): Any 2 systems interconnected as defined by NISPOM 8-700c

C2: Command and Control

C3: Command, Control, and Communications

C3I: Command, Control, Communications and Intelligence

C4: Command, Control, Communications and Computers

CAN: Computer Network Attack

DCID: Director Central Intelligence Directive

DNI: Director of National Intelligence

FIPS: Federal Information Processing Standard

FISMA: Federal Information Security Management Act

I&A: Identification and Authentication

IP: Internet Protocol

NIST: National Institute of Standards and Technology

PIV: Personal Identity Verification

STE: Secure Terminal Equipment

VoIP: Voice over Internet Protocol

VPN: Virtual Private Network

WAN: Wide Area Network

WAP: 1. Wireless Access Point, 2. Wireless Application Protocol

WEP: Wired Equivalent Privacy

WPA2: Wi-Fi Protected Access - 2

XML: Extensible Markup Language