U.S. NUCLEAR REGULATORY COMMISSION MANAGEMENT DIRECTIVE (MD)

MD 12.0	GLOSSARY OF SECURITY TERMS	DT-22-12
Volume 12:	Security	
Approved By:	Jennifer M. Golder, Director Office of Administration	
Date Approved:	October 13, 2022	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of Administration Division of Facilities and Security	
Contact Name:	Denis Brady	Rafael Alequin

EXECUTIVE SUMMARY

Management Directive (MD) 12.0, "Glossary of Security Terms," provides U.S. Nuclear Regulatory Commission staff with definitions for security terms related to Volume 12 of the MD System.

This MD is revised to incorporate necessary changes due to Executive Order 13526, "Classified National Security Information," December 29, 2009; Executive Order 13556, "Controlled Unclassified Information (CUI) Program," November 4, 2010; and updating terms relating to security operations (e.g., physical security, information security, personnel security, cybersecurity, and communications security).

TABLE OF CONTENTS

I. APPLICATION

This Glossary applies to all management directives (MDs) in Volume 12, "Security."

II. GLOSSARY

The following definitions are written from the viewpoint of their specialized meaning in security documents.

Access

The ability or opportunity to gain knowledge of classified or particular information.

Access Authorization

An administrative determination that an individual (including a consultant) is—

1. Employed by, or is an applicant for employment with the NRC, NRC contractors, agents, and licensees of the NRC, or other person designated by the Executive Director for Operations (EDO); and
2. Eligible for access to certain categories of non-public information, such as Restricted Data (RD), Formerly Restricted Data (FRD), National Security Information (NSI), and some types of controlled unclassified information (CUI).

Access Risk

The level of Residual Risk that has been determined to be a reasonable level of potential loss/disruption for a specific information technology (IT) system. This also can include assessments of physical protection systems or equipment important to security.

Adequate Computer Security

Security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and available protections through the application of cost-effective security controls.

Adjudication

Evaluation of pertinent data contained in a background investigation and other relevant reports. The evaluation process is used to determine either or both of the following:

1. Whether an individual is eligible for access to classified or controlled unclassified information (CUI),
2. Whether an individual is suitable for Federal employment.

Administrative Computer User

1. Individual who has either the ability to set “access rights” for users on a given system or to manage technical aspects of the system.
2. Sometimes referred to as a system or network administrator or privileged user.

Administrative Security

1. The management constraints, operational procedures, and supplemental controls established to provide an acceptable level of protection for controlled unclassified information (CUI) data.

2. See also Computer Security, Communications Security, Data Security, Physical Security, Teleprocessing Security, and Transmission Security.

Advanced Encryption Standard (AES)

1. Specifies a Federal Information Processing Standards Publications (FIPS, PUBS)-approved cryptographic algorithm that can be used to protect electronic data.
2. The advanced encryption standard (AES) algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.
3. Encryption converts data to an unintelligible form called ciphertext. Decrypting the ciphertext converts the data back into information technology (IT) original form, called plain text.
4. This standard may be used by Federal departments and agencies when an agency determines that sensitive (unclassified) information requires cryptographic protection.
5. AES replaced Data Encryption Standard.

Agency Communications Security (COMSEC) Manager

1. Individual designated by proper authority to be responsible for the receipt, transfer, accounting, protecting, and destruction of communications security (COMSEC) material assigned to a COMSEC account.
2. For more information, see MD 12.4, “NRC Communications Security (COMSEC) Program.”

Alternate COMSEC Manager

1. Individual designated by proper authority to perform the duties of the communications security (COMSEC) manager during the temporary absence of the COMSEC manager.
2. For more information, see MD 12.4, “NRC Communications Security (COMSEC) Program.”

Application Software

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

Application System

The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures (automated or manual) to achieve a specific objective or function.

Asymmetric Cryptography Keys

Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Asymmetric-Key Cryptography

A cryptographic system where users have a private key that is kept secret and used to generate a public key, which is freely provided to others. Users can digitally sign data with their private key and the resulting signature can be verified by anyone using the corresponding public key. Also known as a Public-key cryptography.

Attack Pathway

Pathway (including physical access, wired connectivity or communications, wireless connectivity or communications, supply chain, or portable media and mobile devices) used or that may be used to gain access to a digital device.

Audit

To conduct the independent review and examination of system records and activities in order to—

1. Test for adequacy of system controls,
2. Ensure compliance with established policy and operational procedures, and
3. Recommend any indicated changes in controls, policy, or procedures.

Audit Trail

A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to final result.

Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. The corroboration that a person is the one claimed.

Authorization to Operate

The official management decision given by a Designated Approving Authority (DAA) to—

1. Approve the operation of a system; and
2. Explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Authorized Classifier

1. An individual authorized in writing by appropriate authority to classify, declassify, or downgrade classified information.
2. This term applies to derivative classifiers and original classifiers.

Authorized User

An authenticated user who has been approved to perform a task or access information or resources.

Authorizing Official (AO)

Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.

Automatic Declassification

The declassification of information based solely upon the following:

1. The occurrence of a specific date or event as determined by the original classification authority, or
2. The expiration of a maximum time frame for duration of classification established under the applicable Executive Order on classified national security information or other applicable authority.

Bandwidth

1. The rate at which data can be transmitted over a given communications circuit.
2. Usually expressed in either kilobits per second, megabits per second, or gigabytes per second.

Baseline Configuration

A documented set of specifications for an information system, or a configuration item within a system that has been formally reviewed and agreed on at a given point in time, and that can be changed only through change control procedures.

Baseline Configuration Identifier

The unique identifier for a baseline configuration.

Business Impact Analysis (BIA)

1. An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
2. The business impact analysis (BIA) includes a correlation of specific system components with the critical services that these components provide.
3. The main purpose of the BIA is to characterize the effect of a system disruption on the business processes and, therefore, to determine the contingency requirements and priorities.

CCI

See Controlled Cryptographic Item.

Central Office of Record (COR)

1. Office of a Federal department or agency that keeps records of accountable communications security (COMSEC) material held by elements subject to its oversight.
2. For more information see MD 12.4, "NRC Communications Security (COMSEC) Program."

Certification

1. A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; or
2. A declaration by a laptop system owner that the required laptop security controls are implemented, operating as intended, and having the desired effect; or
3. A formal acknowledgment of an individual's knowledge, skills, and abilities with respect to a particular specialty (e.g., certified Safeguards Information designator, Microsoft Certified Systems Engineer); or
4. A formal indication that a facility meets a minimum set of security controls (e.g., a certified Sensitive Compartmented Information Facility (SCIF)).

Chief Information Officer (CIO)

1. Agency official responsible for:
   (a) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired, and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency;
   (b) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and
   (c) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
2. For a complete list of duties, see MD 12.5, "NRC Cybersecurity Program."

Chief Information Security Officer (CISO)

Official responsible for carrying out the Chief Information Officer responsibilities detailed in the Federal Information Security Management Act (FISMA) and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information technology (IT) information system security officers (ISSO). For a complete list of duties, see MD 12.5, "NRC Cybersecurity Program."

Classification Authority

The authorized classifier, the classification guide, or the source document or documents that determine the classification of information.

Classification Guidance

Any instruction or source that prescribes the classification of specific information.

Classification Guide

A documentary form of classification guidance issued by an original classification authority that—

1. Identifies the elements of information regarding a specific subject that must be classified, and
2. Establishes the level and duration of classification for each such element.

Classified Data

Restricted Data (RD), Formerly Restricted Data (FRD), and National Security Information (NSI) processed or produced by a system that requires protection against unauthorized disclosure in the interest of national security.

Classified Information

1. Information that has been determined pursuant to Executive Order 13526, "Classified National Security Information," or any predecessor or successor Orders, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate information technology (IT) classified status when in document form.
2. Classified information includes the following:
   (a) Restricted Data (RD),
   (b) Formerly Restricted Data (FRD), and
   (c) National Security Information (NSI) processed or produced by a system that requires protection against unauthorized disclosure in the interest of national security.

Classified Interest

Classified information possessed by the NRC, an NRC contractor, or a facility.

Classified System

A system that processes, stores, or transmits classified information.

Collateral Intelligence

Non-sensitive compartmented information (SCI) intelligence.

Commission

The five members of the NRC or a quorum thereof sitting as a body, as provided by Section 201 of the Energy Reorganization Act of 1974, as amended.

Communications Security (COMSEC)

1. Communications security (COMSEC) is a program that certifies cryptographic and other communication security products. COMSEC information is considered especially sensitive because of the need to protect U.S. cryptographic principles, methods, and materials against exploitation.
2. COMSEC includes the following:
   (a) The protection of information while it is being transmitted by telephone, cable, microwave, satellite, or any other means; and
   (b) Cryptographic security, transmission security, emissions security, and physical security of COMSEC material.
3. For more information see MD 12.4, “NRC Communications Security (COMSEC) Program.”

Compilation

An aggregation of pre-existing unclassified items of information, as defined in Executive Order 13526, “Classified National Security Information.”

Compromise

1. Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
2. Disclosure of classified data to persons not authorized to receive that data.
3. A violation of the security policy of a system such that an unauthorized disclosure, modification, or destruction of controlled unclassified information (CUI) has occurred.

Compromising Emanations

1. Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or information systems equipment.
2. See also TEMPEST.

Computer Facility

One or more rooms of a building containing the main elements of an IT system.

Computer Program

The sequence of coded instructions that cause the computer to solve a problem, store or retrieve information, or perform an information technology (IT) operation.

Computer Security Incident

Any observable occurrence in the system, network, or any other electronic device or component that results in, or has the potential to result in, a negative consequence. Computer security incidents include unexplainable system crashes, unauthorized access to sensitive information, including Personally Identifiable Information, unauthorized modification of sensitive information, network protocol attacks, unauthorized use of system privileges, defacement of a web page, execution of malicious code that destroys data, or loss/theft of computer equipment or media.

Computing Resources

1. Computing resources include the following:

   (a) Computers and information technology (IT) resources, including desktop and laptop computers, networks, facilities, printers, scanners, faxes, portable electronic devices (PEDs), electronic media, and printouts.

   (b) Any other IT used to store or process electronic information.

2. The term Computing Resources in this context is related to Information Technology.

COMSEC

See Communications Security.

COMSEC Account

An administrative entity, identified by an account number, responsible for maintaining custody and control of communications security (COMSEC) material.

COMSEC Accounting

Procedures by which control of communications security (COMSEC) material is maintained from time of origin through destruction or final disposition.

COMSEC Equipment

1. Equipment (including software) designed to provide telecommunication security through the following methods:

   (a) Converting information to a form unintelligible to an unauthorized interceptor, and

   (b) Reconverting this information to its original form for authorized recipients.

2. Equipment designed specifically to aid in, or as an essential element of, the conversion process.
3. Communications security (COMSEC) equipment includes the following:
   (a) Cryptoequipment,
   (b) Crypto ancillary equipment,
   (c) Crypto production equipment, and
   (d) Authentication equipment.

COMSEC Facility

The space used for generating, storing, repairing, or using communications security (COMSEC) material. The COMSEC material may be in either physical or electronic form. Unless otherwise noted, the term "COMSEC facility" refers to all types of COMSEC facilities, including telecommunications facilities, and includes platforms such as ships, aircraft, and vehicles.

COMSEC Information

All information concerning communications security (COMSEC) and all COMSEC material.

COMSEC Insecurity

Any occurrence that jeopardizes the security of communications security (COMSEC) material or the secure electrical transmission of National Security Information (NSI) or national security-related information.

COMSEC Manager

The individual designated to be responsible for the receipt, transfer, accountability, safeguarding, and destruction of communications security (COMSEC) material issued to a COMSEC account.

COMSEC Material

1. Communications security (COMSEC) material includes any information in physical form whose intended purpose is one of the following:
   (a) To deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security, or
   (b) To ensure the authenticity of such communications.
2. COMSEC material includes but is not limited to the following:
   (a) COMSEC keying material in any form to protect or authenticate National Security Information (NSI) or national security-related information, which must be transmitted, communicated, or processed by electrical, electromagnetic, electromechanical, or electro-optical means;

(b) Those items that embody, describe, or implement a cryptographic logic; and

(c) Other items produced by or for the U.S. Government for communications security purposes.

COMSEC Measures

All cryptographic, transmission security, emission security, and physical security techniques employed to protect telecommunications.

COMSEC Survey

1. The application of communications security (COMSEC) analysis and assessment techniques to a specific operation, function, or program.
2. Examination and inspection of a physical location to determine whether alterations and modifications are necessary to render it acceptable for the installation and operation of COMSEC equipment.

COMSEC System

The combination of all measures intended to provide communications security for a specific telecommunications system, including the following:

1. Associated cryptographic, transmission, emission, computer, and physical security measures; and
2. The communications security (COMSEC) support system (documentation; doctrine; keying material protection and distribution; and equipment engineering, production, distribution, modification, and maintenance).

COMSEC Training

Teaching of skills related to the following:

1. Communications security (COMSEC) accounting,
2. Use of COMSEC aids, or
3. Use, maintenance, and repair of COMSEC equipment.

Confidential

A security classification that must be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security, damage which the original classification authority is able to identify and/or describe. For more information see MD 12.2, “NRC Classified Information Security Program.”

Confidential Source

Any individual or organization that has provided, is providing, or that may reasonably be expected to provide information to authorized agents of the U.S. Government on matters pertaining or relating to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

Confidentiality

1. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information (44 U.S.C. 3542).
2. A loss of confidentiality is the unauthorized disclosure of information.

Configuration Management

A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

Contingency Plans

1. Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. A Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do.
2. Plans for interim measures to continue operations after a disruption. Interim measures may include the following:
   (a) Relocation of operational capability to an alternate site,
   (b) Recovery of information and functions using alternate equipment, or
   (c) Performance of typically automated functions using manual methods.

Continuous Vetting (CV)

Per Defense Counterintelligence and Security Agency (DCSA), Continuous Vetting (CV) is defined in Executive Order 13764, “Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 to Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters,” by reviewing the background of an individual at any time to determine whether that individual continues to meet applicable requirements. Vetting policies and procedures shall be sustained by an enhanced risk-management approach that facilitates early detection of issues. CV is a real-time review of an individual’s background at any time to determine if they continue to meet their requirements.

Contracting Officials

An employee of the Federal Government who has the authority to bind the Government legally by signing a contractual instrument.

Controlled Area

Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. An area controlled in one of the following ways:

1. The NRC or an NRC contractor exercises administrative and physical control over the area through the use of properly cleared and authorized employees;
2. Guards are stationed to control admittance to the room, building, or structure; or
3. A lock is used to provide reasonable protection against surreptitious entry.

Controlled Cryptographic Item (CCI)

Secure telecommunications or information system, or an associated cryptographic component that is unclassified and handled through the communications security (COMSEC) material control system (CMCS), an equivalent material control system, or a combination of the two that provides accountability and visibility. Such items are marked "Controlled Cryptographic Item," or, where space is limited, "CCI."

Controlled Unclassified Information (CUI) (replaced sensitive unclassified information (SUNSI))

A designation that refers to unclassified information (i.e., information that is not classified National Security Information, Restricted Data, or Formerly Restricted Data) that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. For more information see MD 12.6, "NRC Controlled Unclassified Information (CUI) Program.

Control Zone

1. The space, expressed in feet of radius, surrounding equipment that meets the following requirements:
   (a) The equipment is used to process controlled unclassified information (CUI), and
   (b) The equipment is under sufficient physical and technical control to preclude an unauthorized entry or compromise.
2. Synonymous with Security Perimeter.

COR

See Central Office of Record.

Counterintelligence

1. Counterintelligence means 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.
2. Information gathered and activities conducted to protect against the following:
   (a) Espionage;
   (b) Other intelligence activities;

(c) Sabotage;

(d) Assassinations by or on behalf of foreign powers, organizations, or persons; or

(e) International terrorist activities.

3. Counterintelligence does not include security programs for personnel, physical security, documents, or communications.

Countermeasure

Any action, device, procedure, technique, or other measure that reduces the vulnerability of or threat to a system or information.

Criticality

1. A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.
2. The level of criticality is determined by the organization's need for asset/system availability, integrity, and confidentiality.
3. The level of criticality is directly related to the level of security protection required.

Crosstalk

An unwanted transfer of energy from one communications channel to another.

Crypto Analysis (Cryptanalysis)

1. The study of mathematical techniques for attempting to defeat cryptographic techniques and/or information systems security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself.
2. The steps and operations performed in converting encrypted messages into plain text without the initial knowledge of the key employed in the encryption.
3. In communications security (COMSEC), the purpose of cryptanalysis is to—

(a) Evaluate the adequacy of the security protection, and

(b) Reveal any weaknesses or vulnerabilities in the security protection.

CRYPTO

The marking or designator identifying communications security (COMSEC) keying material used to secure or authenticate telecommunications carrying classified or controlled unclassified information (CUI) U.S. Government or U.S. Government-derived information.

Crypto Equipment

Any equipment employing a cryptographic logic.

Cryptographic

Pertaining to or concerned with cryptography.

Cryptographic System

See Crypto System.

Cryptography

1. The discipline that embodies the principles, means, and methods for the transformation of data to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.
2. The discipline that embodies the principles, means, and methods for providing information security, including confidentiality, data integrity, authentication, non-repudiation, and authenticity.

Crypto Information

Information that would make a significant contribution to the cryptanalytic solution of encrypted text found in a Crypto System.

Crypto Insecurity

An equipment malfunction or an operator error that adversely affects the security of a cryptosystem.

Cryptology

Originally, the field encompassing both cryptography and cryptanalysis. Today, cryptology in the U.S. Government is the collection and/or exploitation of foreign communications and non-communications emitters, known as signals intelligence (SIGINT); and solutions, products, and services, to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of national security telecommunications and information systems, known as Identification and Authentication (I&A).

Crypto Material

All material, including documents, devices, or equipment that—

1. Contains crypto information; and
2. Is essential to the encryption, decryption, or authentication of telecommunications.

Crypto Period

The time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect.

Crypto Security

The component of communications security that results from the provision of technically sound cryptosystems and their proper use.

Crypto System

The associated items of communications security (COMSEC) equipment or material used as a unit to provide a single means of encryption and decryption.

Crypto Variable

See Keying Material.

CUI

See Controlled Unclassified Information.

Custodian

1. A third-party entity that holds and safeguards a user's private keys or digital assets on their behalf. Depending on the system, a custodian may act as an exchange and provide additional services, such as staking, lending, account recovery, or security features.
2. A person who possesses classified information or is otherwise charged with the responsibility to protect classified information.

Cyberattack

Any event in which there is reason to believe that an adversary has committed or caused, or has attempted to commit or cause, an adverse impact on a digital device.

Cybersecurity

The ability to protect or defend the use of cyberspace from cyberattacks.

Damage to the National Security

Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, considering the sensitivity, value, utility, and provenance of that information.

Data

1. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means; and
2. Any representations, such as characters or analog quantities, to which meaning is or may be assigned.

Data Integrity

1. The property that data has not been altered in an unauthorized manner.
2. Data integrity covers data in storage, during processing, and while in transit.

Data Security

The protection of data from accidental or malicious modification, destruction, or disclosure.

Decipher

To convert enciphered text to plain text by means of a cipher system.

Declassification

The authorized change in the status of information from classified information to unclassified information.

Declassification Guide

Written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

Decrypt

To convert encrypted text into its equivalent plain text by means of a cryptosystem.

Dedicated Mode

The operation of an information technology (IT) system such that the central computer facility, the connected peripheral devices, the communications facilities, and all remote terminals are used and controlled exclusively by specific users or groups of users for the processing of particular types and categories of information.

Degauss

1. To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing.
2. To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Degaussing any current generation hard disk (including but not limited to IDE, EIDE, ATA, SCSI, and Jaz) will render the drive permanently unusable since these drives store track location information on the hard drive. Also called “demagnetizing.”

Degausser

An electrical device that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field.

Denial of Service

1. Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose.
2. This includes any action that causes unauthorized destruction, modification, or delay of service.

Derivative Classification

1. The incorporating, paraphrasing, restating, or generating in new form information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information.
2. Derivative classification includes the classification of information based on classification guidance.
3. The duplication or reproduction of existing classified information is not derivative classification.

Derivative Classifier

1. An individual authorized in writing by appropriate authority within the Office of Nuclear Security and Incident Response (NSIR) to derivatively classify National Security Information (NSI), Restricted Data (RD), and Formerly Restricted Data (FRD).
2. See also Derivative Classification and Authorized Classifier.

Designated Approving Authority (DAA)

Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

Digital Device

A device that stores, processes, or transmits data in a digital (as opposed to an analog) form.

Digital Signature

1. The result of a cryptographic transformation of data that, when properly implemented, provides the services of—
   (a) Origin authentication,
   (b) Data integrity, and
   (c) Signer non-repudiation.
2. A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document.
3. Besides being easily transportable, the digital signature ensures that the content of the message or document is unchanged.
4. When a message is time-stamped, it ensures that its sender cannot easily repudiate it later.
5. A digital signature must have the following attributes:
   (a) Signer authentication

   A signature should indicate who signed a document, message, or record, and should be difficult for another person to produce without authorization.

(b) Document authentication

A signature should identify what is signed, making it impracticable to falsify or alter either the signed matter or the signature without detection.

6. In order for a digital signature to meet the required purpose and attributes, the following must be true:

(a) Digital signature is attributable to a single individual,

(b) Key to produce signature must be known to a single individual,

(c) Key must not be derivable,

(d) Recipient must be able to verify signatory identity with a trusted entity,

(e) Signatory must be aware of the signing act and the implications of that act, and

(f) Alterations to the signed information must be detectable.

Disaster Recovery Plan

A written plan indicating how critical business functions will continue to operate in the event of a disaster.

Document

Any recorded information, regardless of the nature of the medium or the method or circumstances of recording, including but not limited to the following:

1. All handwritten, printed, or typed matter;
2. All painted, drawn, or engraved matter;
3. All sound, magnetic, or electromechanical recordings;
4. All photographic prints and exposed or developed film or still or motion pictures;
5. Automated data processing input, memory, program, or output information or records such as punch cards, tapes, drums, disks, or visual displays; and
6. All optical or laser recordings.

Downgrade

1. An authorized reduction in the level of protection to be provided to specified information (e.g., from a Moderate impact-level down to a Low impact-level).
2. To assign a lower classification than that previously assigned.

Eavesdropping

Interception of a conversation by surreptitious means through use of electronic equipment without the consent of one or more of the participants.

Electronic Controlled Unclassified Information

1. The protection of electronic controlled unclassified information (CUI) from unauthorized disclosure, modification, misuse, loss, or denial of service.
2. Measures and controls that ensure confidentiality, integrity, and availability of system assets including hardware, software, firmware, and information being processed, stored, and communicated.
3. The term Computer Security in this context is related to information technology (IT).

Electromagnetic Emanations

Signals transmitted as radiation through the air and through conductors.

Electronic Device

Devices used for more than storage and include some type of electronic processing. Examples of electronic devices include computers, tablets, smart watches, and cellular phones.

Electronic Media

1. Devices for electronic data storage.
2. Electronic storage options change very quickly and include, but are not limited to, the following:
   (a) Hard drives (both internal and external) and removable drives (e.g., external hard drives),
   (b) Compact disc (CDs),
   (c) Digital Versatile Disc (DVDs),
   (d) Thumb drives,
   (e) Flash memory,
   (f) Floppy disks, and
   (g) Magnetic tapes.

Electronic Signature

1. A method of signing an electronic message that—
   (a) Identifies and authenticates a particular person as the source of the electronic message, and
   (b) Indicates this person's approval of the information contained in the electronic message (Government Paperwork Elimination Act of 1998, Section 1709(1)).
2. A digital signature is a type of electronic signature.

Eligible or Eligibility

An individual's initial and continued eligibility for the following:

1. Access authorization or employment clearance,
2. Unescorted access to nuclear power facilities, or
3. Access to controlled unclassified information (CUI).

Emanation

Unintended signals or noise appearing external to equipment.

Emission Security (EMSEC)

The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from the following:

1. Intercept and analysis of compromising emanations from cryptoequipment, and
2. Information technology systems.

Employment Clearance

1. An administrative determination that an individual is eligible for employment or continued employment pursuant to Subsection 145b of the Atomic Energy Act of 1954, as amended.
2. Individuals eligible for employment clearance include the following:
   (a) NRC employees,
   (b) Applicants for NRC employment,
   (c) Consultants, and
   (d) Other persons designated by the Executive Director for Operations (EDO) of the NRC, or the Commission.

Encode

To convert plain text into unintelligible form by means of a code system.

Encryption

1. The mathematical processing of information so that the information can only be decoded and read by someone who has the correct decoding key.
2. Encryption protects information in storage as well as in transit.
3. If a third party intercepted or obtained encrypted information, this person would not be able to read it unless they also had the key.
4. Unencrypted data is called plain text.
5. Encrypted data is referred to as cipher text.

6. Two basic types of encryption are commonly used—

   (a) Symmetric encryption, where a single key is used for both encryption and decryption, and

   (b) Asymmetric encryption or public key encryption, where a pair of keys is used—one for encryption and the other for decryption.

Enterprise Architecture (EA)

1. As a practice, Enterprise Architecture is an analytical discipline employed within an organization to comprehensively define and organize the underlying business, information, application, and technology architectures. The goal of Enterprise Architecture is to drive standardization, efficiency, and optimization in the use of the organization's resources as applied to meeting its mission objectives.
2. As an artifact, an Enterprise Architecture is a conceptual blueprint that describes the structure and operation of an organization across business, information, application, and technology architectures.

Erasure

Process intended to render magnetically stored information irretrievable by normal means.

Executable Code

Computer code that has been compiled into binary machine code.

Executive Order 12333

Executive Order 12333, "United States Intelligence Activities," December 4, 1981, is the foundational authority by which the National Security Agency (NSA) collects, retains, analyzes, and disseminates foreign signals intelligence information. The principal application of this authority is the collection of communications by foreign persons that occur wholly outside the United States.

Executive Order 12977

Executive Order 12977, "Interagency Security Committee," October 19, 1995, was issued to improve governmentwide coordination of security initiatives. The order created an Interagency Security Committee (ISC), chaired by the Administrator of General Services, and tasked the committee to develop and evaluate security standards for Federal facilities. The ISC is responsible for establishing policies for the security and protection of Federal facilities and is overseeing the implementation of security measures in Federal facilities.

Executive Order 13526

Executive Order 13526, "Classified National Security Information," December 29, 2009, prescribes a uniform system for classifying, safeguarding, and declassifying National Security Information (NSI), including information relating to defense against transnational terrorism.

Executive Order 13556

Executive Order 13556, “Controlled Unclassified Information,” November 4, 2010, establishes an open and uniform program for which safeguarding or dissemination controls are required or permitted pursuant to and consistent with law, regulations, and governmentwide policies, excluding information that is classified under Executive Order 13526 or the Atomic Energy Act, as amended.

Facility

An educational institution, manufacturing plant, laboratory, office, building or portion thereof used by the following:

1. The NRC or its contractors,
2. Others associated with the NRC, or
3. Any other organization that is part of or associated with the U.S. Government.

Facility Approval

1. A determination by the NRC that classified information is approved to be used, processed, stored, reproduced, transmitted, or otherwise handled at a specific facility or
2. A determination by the NRC that a facility may be used for electronic processing of NRC controlled unclassified information (CUI).

Facility Register

An index of security facilities.

Facility Security Level (FSL)

A categorization based on the analysis of several security-related facility factors that serves as the basis for implementing countermeasures specified in the Interagency Security Committee standards.

Foreign National

Any person who is not a citizen or national of the United States.

Forensic Analysis

Examination of evidence of unapproved activity found in computers, electronic devices, or facilities, such that the evidence can be used for legal purposes.

Formerly Restricted Data (FRD)

1. Formerly restricted data (FRD) is classified information that was removed from the Restricted Data (RD) category by one of the following agencies, in conjunction with the Department of Defense:
   (a) The Atomic Energy Commission,

(b) The Energy Research and Development Administration, or

(c) The Department of Energy.

2. In order to remove classified information from the RD category, one of the above-named agencies and the Department of Defense jointly determined the following:

(a) That the information related primarily to the military use of atomic weapons,

(b) That the information could be adequately safeguarded as National Security Information (NSI), and

(c) That transmission of the data to other countries and regional defense organizations would be restricted. (The same transmission restrictions that apply to RD apply to FRD.)

Fortuitous Conductor

1. Any conductor that may provide an unintended path for signals.
2. Fortuitous conductors include the following:

(a) Cables,

(b) Wires,

(c) Pipes,

(d) Conduits, and

(e) Structural metal work in the vicinity of a radiation source.

Guard

A uniformed individual who is employed for and charged with protecting classified information, personnel, or U.S. Government property.

Hearing Counsel

An NRC attorney assigned by the General Counsel to prepare and administer hearings in accordance with the following:

1. 10 CFR Part 10, “Criteria and Procedures for Determining Eligibility for Access to Restricted Data or National Security Information or an Employment Clearance”;
2. 5 U.S.C. 7532, “Suspension and Removal”; and
3. NRC MD12.3, “NRC Personnel Security Program.”

Hearing Examiner

A qualified attorney appointed by the Director of the Office of Administration (ADM) to conduct a hearing in accordance with the following:

1. 10 CFR Part 10, “Criteria and Procedures for Determining Eligibility for Access to Restricted Data or National Security Information (NSI) or an Employment Clearance”;
2. 5 U.S.C. 7532, “Suspension and Removal”; and
3. NRC MD 12.3, “NRC Personnel Security Program.”

High Water Mark

The highest sensitivity/classification level of any information that has ever been or will be processed by, stored on, or traversed through the system.

Host

A host is any hardware device that has the capability of permitting access to a network through a user interface, specialized software, network address, protocol stack, or any other means. Some examples include, but are not limited to, computers, personal electronic devices, thin clients, and multi-functional devices.

Identification, User

1. The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items (Physical).
2. The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system or secure area (Cyber).

Identification and Authentication (I&A)

The combination of the two processes described below.

1. Identification

   Recognition of an entity by a system, generally by the use of unique machine-readable usernames.

2. Authentication

   Verification of the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

Inadvertent Release of Data

1. A type of incident involving the placement of electronic information on a system that is not authorized to process that level of information.
2. Examples of an inadvertent release of data include the following:

   (a) Placement of controlled unclassified information (CUI) or classified information on a system or device for which it is not approved or

(b) Placement of a higher classification of classified information onto a system or device approved only for lower levels of classified information.

3. “Inadvertent Release of Data” is synonymous with “Spillage.”

Information

1. 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. An instance of an information type.
2. Executive Order 13526, “Classified National Security Information,” defines information as follows: “Information means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that is owned by, is produced by or for, or is under the control of the United States Government.”

Information Assurance (IA)

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.

Information Availability

1. Ensuring timely and reliable access to, and use of, information (44 U.S.C. 3542).
2. A loss of availability is the disruption of access to, or use of, information or an information system.

Information Owner

1. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
2. In an information-sharing environment, the information owner or steward is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with or provided to other organizations.

Information System

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Security Officer

As related to Information Technology, an individual who is—

1. Knowledgeable in security concepts and principles and technical security concepts and principles; and

2. Responsible to the system owner for ensuring that the operational cybersecurity controls are in place, operating as intended, and having the desired effect for a system, program, or enclave.

Information System Security Plan

A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Information Technology (IT)

1. 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 an executive agency.
2. Equipment is used by an executive agency if it is used directly or is used by a contractor under a contract with the executive agency that—
   (a) Requires the use of this equipment, or
   (b) Requires the use of this equipment, to a significant extent, in the performance of a service or the furnishing of a product.

Information Technology (IT) Resources

1. Includes, but is not limited to, hardware, application software, system software, and information (data).
2. Information technology (IT) services include, but are not limited to, the management, operation (including input, processing, transmission, and output), maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

Information Technology (IT) System

1. A compilation of hardware and software that operate to electronically perform a specific task or set of tasks.
2. Information Technology System is synonymous with Computer System.

Information Technology (IT) System Facility

One or more rooms (e.g., Two White Flint Computer Room, local area network (LAN) equipment rooms), generally contiguous, containing the equipment of an IT system.

Integrity

1. “Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity…” (44 U.S.C. 3542 (b)(1)(A)).
2. A loss of integrity is the unauthorized access, modification, or destruction of information.

Intelligence

Foreign intelligence and counterintelligence as defined by Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended, or by a successor order, and/or applicable statute.

Intelligence Activities

All activities that members of the Intelligence Community are authorized to conduct pursuant to law or Executive Order 12333, "United States Intelligence Activities," as amended, December 4, 1981, or a successor order, and/or applicable statute.

Intelligence Community (IC)

The collective members of the U.S. Government identified in or designated pursuant to Section 3(4) of the National Security Act of 1947, as amended, or Section 3.5(h) of Executive Order 12333, "United States Intelligence Activities," as amended, December 4, 1981, and/or applicable statute.

Intelligence Community Members

1. Federal Government agencies, services, bureaus, or other organizations within the executive branch that play a role in the business of national intelligence.
2. Intelligence Community Members include the following:
   (a) The Office of the Director of National Intelligence;
   (b) The Central Intelligence Agency;
   (c) The National Security Agency;
   (d) The Defense Intelligence Agency;
   (e) The National Geospatial-Intelligence Agency;
   (f) The National Reconnaissance Office;
   (g) The other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;
   (h) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;
   (i) The intelligence elements of the Federal Bureau of Investigation;
   (j) The Office of National Security Intelligence of the Drug Enforcement Administration;
   (k) The Office of Intelligence and Counterintelligence of the Department of Energy;
   (l) The Bureau of Intelligence and Research of the Department of State;
   (m) The Office of Intelligence and Analysis of the Department of the Treasury;
   (n) The Office of Intelligence and Analysis of the Department of Homeland Security;

(o) The intelligence and counterintelligence elements of the Coast Guard; and

(p) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community.

Intelligence Information (II)

Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities.

Interagency Security Committee (ISC)

The Interagency Security Committee (ISC), created by Executive Order 12977, collaborates with multiple Federal agencies to establish standards and policies, and monitors compliance to address continuing governmentwide security and protection for nonmilitary federal facilities in the United States.

Internal Security Audit

A security audit related to Information Technology that is conducted by personnel responsible to the management of the organization being audited.

International Assignee

A non-U.S. citizen who is an employee of a foreign regulatory agency or entity, who, by mutual agreement, is assigned to the NRC and receives on-the-job training for a specified period.

Interpretable Code

Computer code where the source language is translated into machine language, one line at a time, and then executed.

Intrusion Detection System (IDS)

1. A security alarm system that uses an ultrasonic, infrared, visible light beam, door contact, vibration-sensitive or other sensor to detect and signal the entry of unauthorized persons into a protected area.
2. Information technology (IT) capabilities that detect by capturing and analyzing network packets. Listening on a network segment or switch, one network-based intrusion detection system (IDS) can monitor the network traffic affecting multiple hosts that are connected to the network segment.

Inventory, COMSEC

1. The physical verification of the presence of each item of accountable communications security (COMSEC) material charged to a COMSEC account and
2. A listing of each item of accountable COMSEC material charged to a COMSEC account.

Inventory Report, COMSEC

1. A report submitted to the National Security Agency (NSA) Central Office of Record (COR) with a copy to the NRC agency COMSEC custodian (NRC COR) attesting to the inventory of accountable communications security (COMSEC) material.
2. For more information, see MD 12.4, "NRC Communications Security (COMSEC) Program."

Information Technology (IT) Coordinator

1. The individual appointed by the office director/regional administrator to serve as liaison between an NRC office and the Office of the Chief Information Officer (OCIO) regarding information technology (IT) resources.
2. The IT Coordinator must approve—
   (a) Requests for network access,
   (b) Access to server-based applications,
   (c) Remote access,
   (d) Software installation,
   (e) Moves or removals of desktops,
   (f) Software or peripherals acquisitions, and
   (g) Desktop upgrades.
3. The IT Coordinator has the following additional responsibilities:
   (a) Communicate changes in IT Coordinator personnel to OCIO,
   (b) Attend OCIO briefings on IT issues,
   (c) Serve as office liaison between office staff and the OCIO to coordinate agencywide software upgrades,
   (d) Inform the OCIO about any changes to the office computing environment, and
   (e) Provide guidance to staff on securing the shared drives for personally identifiable information (PII) and controlled unclassified information (CUI).

Information Technology (IT) Device

1. Any device, machine, or component that attaches to a computer.
2. Examples of devices include disk drive, thumb drive, flash drive, printer, mouse, and modem.
3. Most devices require a program called a device driver that translates human commands into commands that the device can enact.

Information Technology (IT) Media

1. Any storage device that holds digital data and is not considered an information technology (IT) device.
2. Examples of IT media include compact disk, digital video disk, and floppy disk.

Keying Material

A type of COMSEC aid that supplies either encoding means for manual and auto-manual cryptosystems or crypto variables for machine cryptosystems.

"L" Access Authorization

1. Normally based upon a Tier 3 (T3) investigation or equivalent Access National Agency Check with Written Inquiries + Credit Check (ANACI) conducted by the Defense Counterintelligence and Security Agency (DCSA) Office of Personnel Management (OPM), or another Government agency that conducts personnel security investigations.
2. Permits individuals access, on a need-to-know basis, to SECRET and CONFIDENTIAL National Security Information (NSI) or CONFIDENTIAL Restricted Data (RD) not related to broad naval nuclear propulsion program policy or direction.

Least Privilege

1. The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
2. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Limited Official Use (LOU)

Designation applied to certain controlled unclassified information, originated by the Department of State in oral or documentary form, that is to be given limited internal distribution by U.S. Government agencies and their contractors.

Limited Protection

A form of short-term COMSEC protection applied to the electromagnetic or acoustic transmission of national security-related information.

Local Area Network (LAN)

A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.

Logon

The procedure used to establish the identity of the user and the levels of authorization and access permitted.

LOU

See Limited Official Use.

Magnetic Remanence

The residual magnetism that remains on magnetic storage media after degaussing. Magnetic Remanence can also refer to any data remaining on IT storage media after the removal of power.

Malicious Code

1. Malicious code/malware is software designed to infiltrate or damage a computer system without the owner's informed consent.
2. See Trojan Horse.

Malware

Malicious software designed for infiltrating or damaging a digital device, without the user's consent; software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a network or function; or 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 software.

Man-in-the-Middle Attack

An attack on an authentication protocol in which an attacker positions himself between a claimant and verifier so that the attacker can intercept and alter data.

Marking

1. The means used to associate a set of security attributes with objects in a human-readable form, to enable organizational process-based enforcement of information security policies.
2. The physical act of indicating on a classified document the assigned classification, changes in classification, downgrading and declassification instructions, and any limitations on its use.
3. The physical act of indicating on a controlled unclassified information (CUI) document the assigned category, changes in the CUI category, and removal from the CUI category.

Master Facility Register

A central index maintained by the Division of Facilities and Security (DFS), Office of Administration (ADM) of all security facilities of the NRC, NRC contractors, and other organizations and persons associated with the NRC program.

Mobile Code

Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.

Multiple Sources

Two or more source documents, classification guides, or a combination of both.

National Declassification Center

A sector of the National Archives established to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training regarding the declassification of records determined to have permanent historical value.

National Security

The national defense or foreign relations of the United States, as defined in Executive Order 13526, “Classified National Security Information.”

National Security Council Information (NSCI)

Classified information contained in the following:

1. Any document prepared by or intended primarily for use by the National Security Council (NSC), its interagency groups as defined in National Security Decision Directive-2 (NSDD-2), dated January 12, 1982, or its associated committees and groups; and
2. Deliberations of the NSC or its interagency groups, as defined in NSDD-2, or its associated committees and groups.

National Security Information (NSI)

Information that has been determined pursuant to Executive Order 13526, “Classified National Security Information,” or any successor order, and/or applicable statute, to require protection against unauthorized disclosure and that is so designated.

National Security-Related Information

Unclassified information related to the national defense or foreign relations of the United States.

National Security System

1. Any information system (including any telecommunications system) that is used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency. Either 1(a) or 1(b) must apply.

   (a) The function, operation, or use of the information system—

      (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.

   (b) The information system is protected at all times pursuant to classified procedures established in accordance with an Executive Order or an Act of Congress. The procedures are classified in the interest of national defense or foreign policy.

2. A national security system does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Naval Nuclear Propulsion Information

Certain unclassified information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear power ships, including the associated nuclear support facilities.

Need-to-Know

1. A determination by a person having responsibility for protecting or holding the sensitive information that a proposed recipient's access to the sensitive information is necessary in the performance of an official and lawful requirement.

2. Knowledge of, possession of, or access to sensitive information, including classified, shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

Network

Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

NSCI

See National Security Council Information.

NSI

See National Security Information.

Occupant Emergency Plan (OEP)

1. A facility-specific document that describes the actions that occupants should take to ensure their safety if a fire or other emergency situation occurs.
2. The Occupant Emergency Plan (OEP) reduces the threat to personnel, property, and other assets within the facility in the event of an incident inside or immediately surrounding a facility by providing facility-specific response procedures for occupants to follow.

Optical Storage Media

Media that uses a source of coherent light—usually a semiconductor laser—to read and write the data, usually to an optical disk.

Original Classification

An initial determination that, in the interest of national security, information requires protection against unauthorized disclosure.

Original Classification Authority

An individual authorized by the NRC Chairman or a designated official to classify information that has not been classified previously by another classification authority.

Original Classifier

1. An individual authorized in writing by the appropriate authority to originally classify National Security Information (NSI).
2. See Authorized Classifier.

Page Check

A check of the pages contained within an item of accountable communications security (COMSEC) or Top Secret material to ascertain that no pages are missing, duplicated, or defective.

Passive Electronic Media

1. Electronic media that simply provides a container for information storage but does not have the ability to manipulate the information in any way.
2. Examples of passive electronic media include a compact disc (CD), a digital versatile disc (DVD), and a magnetic tape.

Password

Protected and private string of letters, numbers, and special characters used to authenticate an identity or to authorize access to data.

Peer-to-Peer (P2P)

1. A network technology that relies primarily on participating computers rather than servers to provide both computing power and information storage.
2. Peer-to-Peer (P2P) is used primarily for ad hoc or unplanned connections between the participating computers and their users.

Personally Identifiable Information (PII)

1. Information that can be used to identify or contact a person uniquely and reliably or can be traced back to a specific individual.
2. Personally identifiable information (PII) is a person's name, in combination with any of the following information:
   (a) Relatives' names,
   (b) Postal address,
   (c) Email address,
   (d) Home or cellular telephone number,
   (e) Personal characteristics,
   (f) Social Security number,
   (g) Date or place of birth,
   (h) Mother's maiden name,
   (i) Driver's license number,
   (j) Bank account information,
   (k) Credit card information, or
   (l) Other information that would make the individual's personal identity easily traceable.
3. Note that personal identity is distinct from an individual's professional identity; that is, an employee's name, title, work telephone number, official work location, and work email address are not considered to be PII.
4. PII is not information related to the workplace, such as the work address, work phone number, or work email address.

Personnel Security

The procedures established to ensure that all personnel who have access to National Security Information (NSI) and controlled unclassified information (CUI) have met all investigative requirements and have been granted appropriate clearances.

Physical Security

Active and passive measures designed to deter and prevent unauthorized access to personnel, equipment, facilities, information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity.

PKI

See Public Key Infrastructure.

PKI Certification Authority

A trusted entity that issues and revokes public key certificates and provides public key certificate status information.

PKI Registration Authority

An entity that is trusted by the certification authority to vouch for the identity of users.

Plain Text

Intelligible text or signals that have meaning and that can be read or acted upon without the application of any decryption.

Portable Electronic Device (PED)

Electronic devices having the capability to store, record, and/or transmit text, images/video, or audio data. Examples of such devices include, but are not limited to—pagers, laptops, cellular telephones, radios, compact disc and cassette players/recorders, portable digital assistant, audio devices, watches with input capability, and reminder recorders.

Portable Mass Storage Device

Examples of portable mass storage devices include flash memory device (e.g., Flash Drive, Pen Drive, Key Drive, Thumb Drive, Jump Drive), compact flash, solid-state USB hard drive (e.g., Sony Micro Vault), and Zip disk.

Privileged User

1. A user who is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
2. A person with either limited or unlimited privileged access to a computing resource, such as a system administrator or information system security officer.
3. A privileged user may use and access privileged information on all or part of the computing resource.
4. A privileged user may alter or bypass some or all of the security controls on a computing resource.

Proprietary Information

1. Trade secrets, privileged or confidential research, development, commercial, or financial information exempt from mandatory disclosure under the NRC's regulations in 10 CFR Title I, including, but not limited to the following:

   (a) 10 CFR Part 2, "Rules of Practice for Domestic Licensing Proceedings and Issuance of Orders."

   (b) 10 CFR 2.336, "General Discovery."

   (c) 10 CFR 2.390, "Public Inspections, Exemptions, Requests for Withholding."

   (d) 10 CFR Part 9, "Public Records," Section 9.17, "Agency Records Exempt from Public Disclosures," and

   (e) 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

   (f) Material and information relating to or associated with a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that has been clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information. Generally, information that is available to the general public would not qualify as proprietary.

2. Other information that is submitted in confidence to the NRC by a foreign source and determined to be unclassified by the NRC must be marked as proprietary information.

3. See controlled unclassified information (CUI).

Protected Area

The "protected area" is any area encompassed by physical barriers and to which access is controlled.

Protected Distribution System

See Protected Wireline System.

Protected Wireline System

1. A wireline or fiber-optics system that includes adequate acoustical, electrical, electromagnetic, and physical safeguards to permit its use for the transmission of unencrypted classified information.

2. Synonymous with Protected Distribution System.

Protective Packaging

Packaging techniques for keying material that discourage penetration, reveal that a penetration has occurred, or inhibit viewing or copying of keying material before the time it is exposed for use.

Public Key Infrastructure (PKI)

1. The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates.
2. The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.
3. A method of providing high-level encryption, authentication, and digital signature capability based on public key certificates.

Purging

1. A method of sanitization that applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.
2. Rendering stored information unrecoverable. (See Sanitizing.)

"Q" Access Authorization

1. A "Q" access authorization is normally based upon a Tier 5 (T5) investigation conducted by the Defense Counterintelligence and Security Agency (DCSA) or another Government agency that conducts personnel security investigations.
2. This authorization permits individuals to have access, on a need-to-know basis, to Top Secret, Top Secret RD, Secret, Secret RD, Confidential, and Confidential RD.

Raw Intelligence (Sensitive Compartmented Information and Collateral)

1. Intelligence information on which there is little or no processing or evaluation to assess its reliability, factual content, or credibility.
2. Documents containing raw intelligence may or may not identify intelligence sources and methods.

Reciprocity

1. The policy of accepting a prior favorable investigation or personnel security determination performed by another agency of the Federal Government.
2. The prior action must meet acceptable investigative scope and standards.

3. The policy of reciprocity is set forth by Executive Order 12968, “Access to Classified Information.”

Reconstitution

1. The process that takes place following recovery from a contingency and includes activities to access a system and for returning the information system to its original functional state before contingency plan activation.
2. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations.
3. Reconstitution also includes an assessment of the fully restored information system capability, a potential system reauthorization, and the necessary activities to prepare the system against another disruption, compromise, or failure.

Records

1. All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the U.S. Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them.
2. Library and museum material made or acquired and preserved solely for reference or exhibition purposes. Extra copies of documents preserved only for convenience of reference and stocks of publications and of processed documents are not included “Definition of Records” (44 U.S.C. 3301).

Records Management

The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations (44 U.S.C. 2901(2)).

Recovery Procedures

The actions necessary to restore a system’s computational capability and data files after a system failure or penetration.

Red/Black Concept

The concept that telecommunications circuits, components, equipment, and systems that handle classified, plain-language information in electrical signal form (Red) be separated from those that handle encrypted or unclassified information (Black).

Registered Initials

One of the elements in an identification technique for restricting access to a computer database or terminal to the individual whose initials have been recorded (registered) with the computer software that restricts access.

Registration Authority

See PKI Registration Authority.

Reliability

The probability of a given system performing its mission adequately for a specified period of time under the expected operating conditions.

Remanence

1. The residual magnetism that remains on magnetic storage media after degaussing.
2. Can also mean any data remaining on IT storage media after removal of the power.

Remote Access

1. Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the internet).
2. Access for authorized users external to an enclave established through a controlled access point at the enclave boundary.

Residue

Electronic data left in storage after information processing operations are complete but before degaussing or overwriting has taken place.

Restricted Data (RD)

1. All data concerning the following:
   (a) Design, manufacture, or use of atomic weapons;
   (b) The production of special nuclear material; or
   (c) The use of special nuclear material in the production of energy.
2. Restricted data (RD) does not include data declassified or removed from the RD category in accordance with Section 142 of the Atomic Energy Act of 1954, as amended.

Risk

1. A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of—
   (a) The adverse impacts that would arise if the circumstance or event occurs and

(b) The likelihood of occurrence.

2. The probability that a particular threat will adversely impact an information system by exploiting a particular vulnerability.

3. Information technology (IT)-related risk is the net mission impact considering the following:

   (a) The probability that a particular threat source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability; and

   (b) The resulting impact if this should occur.

4. IT-related risks arise from legal liability or mission loss due to the following:

   (a) Unauthorized (malicious or accidental) disclosure, modification, or destruction of information;

   (b) Unintentional errors and omissions;

   (c) IT disruptions due to natural or human-made disasters; and

   (d) Failure to exercise due care and diligence in the implementation and operation of the IT system.

Risk Acceptance

The explicit or implicit decision to not take an action that would affect all or part of a particular risk.

Risk Analysis

1. The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact.

2. Part of risk management and synonymous with Risk Assessment.

Risk Assessment

1. The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

2. The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences.

3. Part of risk management and synonymous with Risk Analysis.

Risk Evaluations

Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk Management

1. The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes—
   (a) The conduct of a risk assessment,
   (b) The implementation of a risk mitigation strategy, and
   (c) Employment of techniques and procedures for the continuous monitoring of the security state of the information system.
2. The process of identifying, controlling, and mitigating risks related to information systems.
3. It includes risk assessment, cost-benefit analysis, and the selection, implementation, testing, and evaluation of security protections.
4. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.

Safeguarding

1. Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system.
2. Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.
3. Measures and controls that are prescribed to protect classified information.

Safeguards Information (SGI)

1. Safeguards Information (SGI) identifies the detailed security measures of licensee or an applicant that are designed to do the following:
   (a) Protect source, byproduct, or special nuclear material, and
   (b) Protect the physical location of certain plant equipment that is vital to safety of production/ utilization facilities.
2. Safeguards Information (SGI) must be protected pursuant to Section 147 of the Atomic Energy Act of 1954, as amended.
3. A more detailed definition of SGI is outlined in 10 CFR 73.2.

4. SGI is a CUI Specified category of controlled unclassified information (CUI) that is identified in the NARA CUI Registry, and the applicable CUI marking is "CUI//SP-SGI." SGI in the NRC's possession, or in the possession of another federal agency, qualifies as CUI, while SGI in a licensee or applicant's possession may, or may not, qualify as CUI, depending on the circumstances. In general, SGI regarding an applicant or licensee's own facilities or materials is not considered CUI when in the possession of the applicant or licensee, but such SGI remains subject to the protection requirements under the Atomic Energy Act of 1954 and the NRC's implementing regulations in 10 CFR Part 73.
5. For more information, see MD 12.7, "NRC Safeguards Information Security Program," and MD 12.6, "NRC Controlled Unclassified Information (CUI) Program."

Safeguards Information (SGI) Local Area Network (LAN) and Electronic Safe (SLES) System

1. The Safeguards Information (SGI) Local Area Network (LAN) and Electronic Safe (SLES) System is a secure electronic repository for Safeguards Information (SGI) records created and received by the NRC.
2. SLES has two components: Safeguards Information Local Area Network (SGI LAN) and Electronic Safe (E-Safe).
3. SLES provides secure access to SGI (access is through secure network and connected cables).
4. E-Safe is the agency's official record keeping system for SGI.

Safeguards Information - Modified Handling (SGI-M)

1. According to 10 CFR 73.2, "Safeguards Information – Modified Handling," is defined as follows: "The designation or marking applied to Safeguards Information which the Commission has determined requires handling requirements modified from the specific Safeguards Information handling requirements that are applicable to Safeguards Information needing a higher level of protection." Within the confines of the NRC, staff and contractors must safeguard and protect SGI-M in a manner identical to SGI.
2. Like SGI, SGI-M in the possession of the NRC or another federal agency will qualify as CUI, while SGI-M in the possession of a non-executive branch entity, such as a licensee or applicant, may or may not qualify as CUI, depending on the circumstances. The CUI marking used for SGI-M is the same marking that is also used for SGI (i.e., "CUI//SP-SGI").
3. For more information, see MD 12.7, "NRC Safeguards Information Security Program," and MD 12.6, "NRC Controlled Unclassified Information (CUI) Program."

Sanitizing

1. Removing information from media so that it cannot be recovered. It includes removing all information labels, markings, and activity logs. (See Purging.)
2. The term Sanitizing in this context is related to Information Technology (IT).

Scavenging

Searching through residue for the purpose of data acquisition.

SCI

See Sensitive Compartmented Information.

SECRET

1. "Secret" is a security classification that must be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security, damage which the original classification authority is able to identify and/or describe.
2. For more information, see MD 12.2, "NRC Classified Information Security Program."

Secret Internet Protocol Router Network (SIPRNet)

1. Secret Internet Protocol Router Network (SIPRNet) is a system of interconnected computer networks used by the U.S. Department of Defense (DOD) and the U.S. Department of State to transmit classified information (up to and including information classified SECRET) through the Transmission Control Protocol/Internet Protocol (TCP/IP) suite in a completely secure environment.
2. SIPRNet also provides services such as hypertext document access and electronic mail.
3. SIPRNet is the DOD's classified version of the civilian internet together with its counterpart, the Top Secret and sensitive compartmented information (SCI) Joint Worldwide Intelligence Communications System (JWICS).
4. The DOD Non-Classified Internet Protocol Router Network (NIPRNet) is used to exchange unclassified information.

Secure Operating System

An operating system that effectively controls hardware and software functions in order to provide the level of protection appropriate to the value of the data and resources managed by the operating system.

Secure Telecommunications Facility

A telecommunications facility that employs cryptomaterial to protect the transmission of National Security Information (NSI).

Security Area

A physically defined space containing classified information and subject to physical protection and personnel access controls.

Security Assessment

1. The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
2. The comprehensive evaluation of the technical and nontechnical security features of IT systems and other protections made in support of the authorization process that establishes the extent to which a particular design and implementation meet a specified set of security requirements.
3. The term Security Assessment in this context is related to Information Technology (IT).

Security Assurance

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

Security Clearance

1. The term Security Clearance in this context relates to an NRC access authorization.
2. See Access Authorization.

Security Control Assessment

The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Security Control Assessor (Formerly Certification Authority)

The individual, group, or organization responsible for security control assessment.

Security Controls

1. Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system.
2. Management, operational, and technical controls (i.e., protections and countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Event

1. Any observable occurrence in a network or system.
2. Occurrence not yet assessed that may affect the performance of an information system.
3. Related to Information Technology (IT).

Security Facility Approval

See Facility Approval.

Security Facility

Any facility that has been approved by the NRC or another Government agency for using, processing, storing, reproducing, transmitting, or otherwise handling classified information.

Security Importance Rating

1. An alphabetical letter designating the relative importance to the national security of an activity that involves classified information.
2. These ratings are assigned to security facilities and to individual classified interests within security facilities, as set forth in MD 12.1, “NRC Facility Security Program.”

Security Incident

Any event, act, or omission involving a failure to comply with written NRC security requirements, or applicable policies or procedures. A security incident also includes a computer security incident, which is the failure to comply with applicable computer security requirements and/or applicable facility physical protection requirements. All security events will be referred to as a “security incident” until determined otherwise.

Security Infraction

A security incident that does not result in an actual or possible compromise of classified information covered under the requirements of Executive Order 13526, its implementing directives, or successor. A security infraction is usually a minor incident or administrative error in the safeguarding of classified information that does not result in the compromise of such information or the likelihood of such compromise is remote. Examples include leaving a classified storage container open, leaving a classified document unprotected, failing to properly safeguard combinations, improper transmission of classified documents, failure to report known or suspected security incidents involving classified information, failure to properly escort uncleared persons within a security area, and processing or communicating classified information in areas not approved by the Division of Facilities and Security, Office of Administration.

Security Perimeter

See Control Zone.

Security Plan

1. A document that meets the following criteria.
   (a) The document is prepared by one of the following:
      (i) An NRC office, division, or region;
      (ii) An NRC contractor;
      (iii) A consultant;

(iv) A licensee; or

(v) A licensee-related organization.

(b) The document describes the following:

(i) The security procedures followed by the organization or individual;

(ii) Measures used to safeguard classified interests, sensitive unclassified interests, or both; and

(iii) Measures used to ensure the security education of the employees.

2. The term Security Plan includes security plans for foreign assignees.

3. See Information System Security Plan.

Security Policy

The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Proposal System

1. A document that outlines a system (e.g., telecommunications or an information technology (IT) system) and the security measures to protect sensitive or classified information processed, produced, or communicated by the system.

2. Once approved, the proposal becomes a plan.

Security Survey

1. An onsite examination of a security facility by an NRC security representative.

2. The examination is conducted to accomplish the following:

(a) Assess the devices, equipment, and procedures employed within an organization or facility;

(b) Safeguard classified information, controlled unclassified information, or both; and

(c) Protect personnel and property.

Security Violation

A security incident that could reasonably be expected to result in the actual or possible unauthorized disclosure of classified information covered under the requirements of Executive Order 13526.

Sensitive Application

An application that requires a degree of protection because it processes sensitive data (i.e., administrative, personnel, financial, or national security data) or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation.

Sensitive Compartmented Information (SCI)

1. A subset of Classified National Intelligence concerning or derived from intelligence sources, methods or analytical processes that is required to be protected within formal access control systems established by the Office of the Director of National Intelligence.
2. All information and materials requiring special community controls indicating restricted handling within present and future community intelligence collection programs and their end products.
3. These special community controls are formal systems of sources and methods and analytical procedures of foreign intelligence programs.
4. The term does not include Restricted Data (RD) as defined in Section 11, Public Law 585, Atomic Energy Act of 1954, as amended (42 U.S.C. 2014).

Sensitive Compartmented Information Facility (SCIF)

An accredited area, room, group of rooms, or installation in which sensitive compartmented information (SCI) may be stored, used, discussed, or processed.

Sensitive Information

A generic term used to identify information designated as Classified National Security Information (NSI) or Controlled Unclassified Information (CUI).

Sensitive System

A system or network that stores, processes, or transmits sensitive information.

Sensitivity Level

A designation associated with information that indicates the following:

1. The amount of harm that can be caused by the compromise of the confidentiality, integrity, or availability of that information;
2. Any formal access approvals that should be granted before the granting of access to that information; and
3. Any specific handling restrictions placed on that information.

Shared Logic

In word processing, an arrangement in which two or more proximate workstations share common facilities.

Shielded Enclosure

An area (room or container) specifically designed to attenuate electromagnetic radiation or acoustic emanations originating either inside or outside the area.

Significant Information of Intelligence Value

Information useful to a foreign country or to a terrorist preparing or executing an operational plan that is contrary to the best interests of the United States.

Smart Card

1. A plastic card, the size of a credit card, containing an embedded integrated circuit or a chip that can generate, store, or process data.
2. The card can be used to facilitate various authentication technologies also embedded on the same card.

Software Security

General purpose (executive, utility, or software development tools) and applications programs or routines that protect data handled by a system.

Source Document

An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Special Access Program (SAP)

A program established, under Executive Order 13526, Section 4.3, for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information classified at the same classification level.

Spillage

1. A type of incident where electronic information is placed on a system that is not authorized to process that level of information.
2. Examples include placement of controlled unclassified information (CUI) (includes within its scope Safeguards Information (SGI)), or classified information on the NRC LAN/wide area network (WAN), or a device not approved for CUI, or classified information, or placement of a higher classification of information onto a system or device approved only for lower levels of classified information.
3. Spillage is synonymous with Inadvertent Release of Data.

Spread-Spectrum

1. Telecommunications techniques in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information.
2. Frequency hopping, direct sequence spreading, time scrambling, and combinations of these techniques are forms of spread spectrum.

Spread-Spectrum Mobile Communication

Wireless telephones that transmit voice communication across multiple frequencies and employ spread-spectrum mobile communication.

Stand-Alone System

A system that requires no other piece of equipment with it to complete its own operation. It can, and usually does, operate independently (e.g., a personal computer or a word processor).

Storage Medium

Any device or recording medium into which data can be stored and held until some later time and from which the entire original data can be obtained.

Supply Chain Risk

The risk that any person may sabotage, maliciously introduce unwanted functionality, extract data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement of covered articles so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the covered articles or information stored or transmitted by or through covered articles.

Supply Chain Risk Assessment

A systematic examination of supply chain risks, likelihood of their occurrence, and potential impacts.

Supply Chain Risk Information

Includes, but is not limited to, information that describes or identifies—

1. Functionality and features of covered articles, including access to data and information system privileges;
2. The user environment where a covered article is used or installed;
3. The ability of a source to produce and deliver covered articles as expected;
4. Foreign control of, or influence over, a source or covered article (e.g., foreign ownership, personal and professional ties between a source and any foreign entity, legal regime of any foreign country in which a source is headquartered or conducts operations);
5. Implications to Government mission(s) or assets, national security, homeland security, or critical functions associated with use of a source or covered article;
6. Vulnerability of Federal systems, programs, or facilities;
7. Market alternatives to the covered source;
8. Potential impact or harm caused by the possible loss, damage, or compromise of a product, material, or service to an organization’s operations or mission;
9. Likelihood of a potential impact or harm, or the exploitability of a system;
10. Security, authenticity, and integrity of covered articles and their supply and compilation chain;

11. Capacity to mitigate risks identified;
12. Factors that may reflect upon the reliability of other supply chain risk information; and
13. Any other considerations that would factor into an analysis of the security, integrity, resilience, quality, trustworthiness, or authenticity of covered articles or sources.

Surreptitious Listening Device

See Wiretapping.

Symmetric Cryptography Key

Key used to both encrypt and decrypt information. Individuals who need access to the information must share the key.

System

A compilation of hardware, software, and firmware that processes electronic information to achieve a particular purpose. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See Classified System and Unclassified System.

System Backup

1. A copy of a program or data file that is kept for reference in case the original is lost or destroyed.
2. Reserve computing capability available in case of equipment malfunction, destruction, or overload.

System Integrity

1. The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
2. See Data Integrity.

System Integrity Study

An examination and analysis of the security measures of an IT system to determine whether any deliberate attempt by personnel or failure of system components could adversely affect the common defense and security.

Technical Surveillance Countermeasures (TSCM) Inspection

Technical inspection of a facility or premises to determine the actual or possible presence of wiretapping or eavesdropping devices.

Technological Attack

An attack that can be perpetrated by circumventing or nullifying hardware and software access control mechanisms rather than by subverting system personnel or other users.

Telecommunications

The transmission between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.

Telecommunications Protection

1. The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, or modification of information in a teleprocessing system.
2. See Teleprocessing Security.

Telecommunications Security

1. The protection that ensures the authenticity of telecommunications.
2. Telecommunications security involves the application of measures that deny unauthorized persons information of value that might be otherwise derived from the acquisition of telecommunications.
3. Telecommunications security includes the following:
   (a) Cryptosecurity,
   (b) Transmission security,
   (c) Emission security, and
   (d) Physical security of communications security material and information.

Telecommunications System Security Proposal

1. A document that outlines a telecommunications system and the security measures to protect controlled unclassified information (CUI) or classified information communicated by the system.
2. Once approved, the proposal becomes a plan.

Teleprocessing

Pertaining to an information transmission system that combines telecommunications, IT systems, and man-machine interface equipment for the purpose of interacting and functioning as an integrated whole.

Teleprocessing Security

1. The protection resulting from all measures designed to prevent deliberate, inadvertent, or unauthorized disclosure, acquisition, manipulation, or modification of information in a teleprocessing system.
2. See also IT Security, Data Security, Communications Security, Transmission Security, and Telecommunications Protection.

TEMPEST

1. A term referring to investigations and studies of compromising emanations.
2. Synonymous with TEMPEST tests and TEMPEST inspections.

TEMPEST-Approved Equipment or Systems

Equipment or systems that have been certified with the requirements of the effective edition of NACSIM 5100, “Tempest Specifications.”

TEMPEST Test

A laboratory or onsite (field) test to determine the nature and amplitude of conducted or radiated signals containing compromising information.

Temporary Access Authorization

An authorization that permits an individual access to NRC facilities and/or information technology (IT) after a favorable pre-employment review is conducted and before a background investigation is adjudicated.

Terminal Identification

The means used to establish the unique identification of a terminal by a system.

Third Agency Document

A document that—

1. Was originated by personnel of a Government agency or its contractors, by a foreign government, or by an international organization; and
2. Was provided to the NRC by an organization other than the originator.

Threat

Natural or human-made occurrences, individuals, entities, or actions that have or indicate the potential to harm life, information, operations, the environment, or property.

Threat Monitoring

The analysis, assessment, and review of audit trails and other data for the purpose of searching out system events that may constitute violations or may precipitate incidents involving data privacy matters.

Time-Dependent Password

A password that is valid only at a certain time of the day or during a specified interval of time.

Time-Shared System

A system in which available central computer time is shared among several jobs as directed by a scheduling plan or formula.

Top Secret

1. The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security (the highest classification level).
2. For more information see MD 12.2, “NRC Classified Information Security Program.”

Traffic

Messages or voice communications or messages transmitted or received by telecommunications.

Transaction

1. A discrete event between a user and a system that supports a business or programmatic purpose. A Government digital system may have multiple categories or types of transactions, which may require separate analysis within the overall digital identity risk assessment.
2. A sequence of information exchange and related work (such as database updating) that is treated as a unit for the purposes of satisfying a request and for ensuring database integrity.
3. A transaction has to be completed in its entirety for a transaction to be completed and database changes to be made permanent.
4. The term “transaction” in this context is related to Information Technology (IT).

Transmission Security (TRANSEC)

1. The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.
2. See information technology (IT) Security, Data Security, Communications Security, and Teleprocessing Security.

Trojan Horse

1. A computer program that appears to have useful function, but also a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. For example, such a computer program might make a “blind copy” of a sensitive file.
2. See Malicious Code.

Trusted Agent

1. An individual explicitly aligned with one or more registration authority (RA) officers who has been delegated the authority to perform a portion of the RA functions.
2. A trusted agent (TA) does not have privileged access to certification authority system (CAS) components to authorize certificate issuance, certificate revocation, or key recovery.
3. Trusted agents do not have automated interfaces with certification authorities.

TSCM

See Technical Surveillance Countermeasures.

Unauthorized Disclosure

A communication or physical transfer. An event involving the exposure of classified information to an unauthorized recipient entity not authorized access to the information.

Unclassified System

A system that only processes, stores, or transmits unclassified information.

Undocumented noncitizen

An individual who has entered the United States illegally and is deportable if apprehended, or an individual who entered the United States legally but who has fallen "out of status" and is deportable. Formerly known as an “undocumented alien.”

Upgrade

1. An authorized increase in the level of protection to be provided to specified information (e.g., from a Low impact-level to a Moderate impact-level).
2. To raise the classification level of information.

U.S. Citizen

An individual born in the U.S., an individual whose parent is a U.S. citizen, a former non-citizen who has been naturalized as a U.S. citizen, an individual born in Puerto Rico, an individual born in Guam, or an individual born in the U.S. Virgin Islands.

U.S. National

An individual owing permanent allegiance to the United States, including all U.S. citizens, and including some individuals who are not U.S. citizens, including some individuals who were born in American Samoa or the Commonwealth of the Northern Mariana Islands.

User

Individual (general user, non-public user, or a privileged user) or process authorized to access an information system.

User-ID (Identifier)

A unique symbol or character string that is used by a system to identify a specific 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).

Vault

An NRC-approved windowless enclosure constructed with walls, floor, roof, and door(s) that will delay penetration from forced entry.

Vault-Type Room

An NRC-approved room equipped with the following:

1. Combination-locked door and
2. An intrusion detection system (IDS) that activates upon unauthorized penetration of walls, floor ceiling, or openings, or by motion within the room.

Violation (of Law)

Criminal or civil violation of statutes of security interest.

Virus

1. 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 email programs to spread itself to other computers, or even erase everything on a hard disk.
2. The term Virus in this context is related to the term Information Technology.

Vital Area

An area that contains vital equipment.

Vulnerability

1. Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
2. The term Vulnerability in this context is related to the term Information Technology.

Vulnerability Assessment

1. Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
2. The systematic examination of telecommunications to accomplish the following:
   (a) Determine the adequacy of communications security (COMSEC) measures,
   (b) Identify COMSEC deficiencies,
   (c) Provide data from which to predict the effectiveness of proposed COMSEC measures, and
   (d) Confirm the adequacy of these measures after implementation.

Watchman

A person, unarmed and not necessarily uniformed, who provides protection for classified information or U.S. Government property.

Weapons Data

1. Classified information concerning the design, manufacture, or use of atomic weapons or components thereof. This classified information includes the following:
   (a) Theory,
   (b) Development,
   (c) Storage,
   (d) Characteristics,
   (e) Performance, and
   (f) Effects.
2. Weapons data also includes information incorporated in or relating to nuclear explosive devices.

Wide Area Network (WAN)

A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and that is usually spread over a larger geographic area than that of a LAN.

Wi-Fi Hotspot

A physical location offering shared internet access to the public using a wireless LAN.

Wireless Technology

1. Permits the active or passive transfer of information between separated points without physical connection.
2. Active information transfer may entail a transmit and/or receive emanation of energy, whereas passive information transfer entails a receive-only capability.
3. Currently wireless technologies use infrared radiation, acoustic, radio frequency, and optical but, as technology evolves, wireless could include other methods of transmission.

Wireless Telephone

A telephone that uses wireless technology.

Wiretapping or Eavesdropping Device

1. Electronic device designed primarily to surreptitiously intercept communications without the consent of any of the participants.
2. Synonymous with Surreptitious Listening Device.

Wiretapping

The direct or inductive coupling by surreptitious means of an electronic device to lines transmitting communications without the consent of any of the participants.

Working Variable

A crypto variable distributed by a key generation facility for use on a specific interstation call.

III. REFERENCES

Code of Federal Regulations

10 CFR Part 2, “Rules of Practice for Domestic Licensing Proceedings and Issuance of Orders.”

10 CFR Part 9, “Public Records,” Section 9.17, “Agency Records Exempt from Public Disclosures.”

10 CFR Part 10, “Criteria and Procedures for Determining Eligibility for Access to Restricted Data or National Security Information or an Employment Clearance.”

10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants.”

10 CFR Part 73, “Physical Protection of Plants and Materials.”

Executive Orders (E.O.)

12333, “United States Intelligence Activities,” as amended, December 4, 1981.

12958, “Classified National Security Information,” April 17, 1995.

12968, “Access to Classified Information,” August 2, 1995.

12977, “Interagency Security Committee,” October 19, 1995.

13526, “Classified National Security Information,” December 29, 2009.

13556, “Controlled Unclassified Information,” November 4, 2010.

13764, “Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 to Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters.”

National Security Council Documents

National Security Decision Directive-2 (NSDD-2), January 12, 1982.

Nuclear Regulatory Commission Documents

Management Directives (MD)—

12.1, “NRC Facility Security Program.”

12.2, “NRC Classified Information Security Program.”

12.3, “NRC Personnel Security Program.”

12.4, “NRC Communications Security (COMSEC) Program.”

12.5, “NRC Cybersecurity Program.”

12.6, “NRC Controlled Unclassified Information (CUI) Program.”

12.7, “NRC Safeguards Information Security Program.”

United States Code

Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.).

Definition of Records (44 U.S.C. 3301).

Energy Reorganization Act of 1974, as amended (42 U.S.C. 5801 et seq.).

Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. 3541 et seq.).

Government Paperwork Elimination Act of 1998 (44 U.S.C. 3504 et seq.).

National Security Act of 1947, as amended.

Privacy Act (5 U.S.C. Section 552 a).

Suspension and Removal (5 U.S.C. 7532).