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

MD 12.0	GLOSSARY OF SECURITY TERMS	DT-14-17
Volume 12:	Security	
Approved by:	Cynthia A. Carpenter Director, Office of Administration	
Date Approved:	July 1, 2014	
Expiration Date:	July 1, 2019	
Issuing Office:	Office of Administration Division of Facilities and Security	
Contact Name:	Calvin Byrd 301-415-7402	

EXECUTIVE SUMMARY

Management Directive (MD) 12.0 provides the NRC staff with definitions for security terms related to Volume 12 of the MD System.

This MD is being revised to incorporate changes necessary due to new Executive orders and national security guidance, including Executive Order 13526, "Classified National Security Information," dated December 29, 2009.

TABLE OF CONTENTS

I. APPLICATION

This Glossary applies to all management directives (MDs) contained within 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; and
2. Eligible for access to information that is not publicly available, including but not limited to Sensitive Unclassified Non-Safeguards Information, Safeguards Information, Restricted Data, Formerly Restricted Data, and National Security Information.

Access National Agency Check and Inquiry (ANACI)

An Office of Personnel Management background investigation product consisting of a National Agency Check, employment checks, education checks, residence checks, reference checks, and local law enforcement checks.

Access Privilege

The particular Information Technology (IT) access permission (i.e., read, write, append, execute, delete, create, modify) granted to a subject in relation to an object.

Accreditation

Using an older methodology, accreditation was the formal approval to operate an IT system as granted by the accrediting authority. The accreditation process has been replaced by the authorization process by the appropriate authority.

Adequate Computer Security

1. Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information.
2. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.
3. Computer security measures required by applicable authority.

Adjudication

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

1. Whether an individual is eligible for access to classified or sensitive information and/or
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 sensitive 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 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 its original form, called plaintext.
4. This standard may be used by Federal departments and agencies when an agency determines that sensitive (unclassified) information (as defined in Pub. L. 100-235) requires cryptographic protection.
5. AES replaced Data Encryption Standard.

Agency Communications Security (COMSEC) Manager

Individual designated by proper authority to be responsible for the receipt, transfer, accounting, protecting, and destruction of COMSEC material assigned to a COMSEC account.

Alien

An individual who is not a U.S. citizen or U.S. national.

Alternate COMSEC Manager

Individual designated by proper authority to perform the duties of the COMSEC manager during the temporary absence of the COMSEC manager.

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.

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 of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of events or changes in computing environment.

Authenticated User

Any user that authenticates to NRC systems or networks and who is authorized by the NRC for system or network access.

Authentication

1. The act of identifying or verifying a security measure designed to establish the validity of a transmission, message, user, or originator; or
2. A means of verifying an individual's authorization to receive specific categories of information.

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.

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.

Automated Information System (AIS)

An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

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

The composition of an IT product that has been approved for release into operations.

Baseline Configuration Identifier

The unique identifier for a baseline configuration.

Business Area Leader

A business area leader is an office director, a regional administrator, or a deputy executive director responsible for an NRC business area, such as nuclear reactor regulation. A business area consists of multiple specific functions required to achieve the mission responsibilities of the business area. Each function has a different criticality in performing the mission; performance of each of those functions may require one or more IT system. Identification of the IT systems associated with each function allows the business area leader to determine the criticality of each IT system upon which the business area relies. Each IT system must meet the needs of the business area with the highest dependence upon the IT system.

Business Impact Analysis (BIA)

1. An analysis of system requirements, system processes, and interdependencies required to perform a business function.
2. The 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)

Office of a Federal department or agency that keeps records of accountable COMSEC material held by elements subject to its oversight.

Certification

1. A laptop system owner declaration that the required laptop security controls are implemented, operating as intended, and having the desired effect;
2. A formal acknowledgement 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
3. 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)

The NRC management official who is responsible for the following:

1. Planning, directing, and overseeing the delivery of centralized information technology infrastructure, applications, and information management services; and
2. The development and implementation of plans, architecture, and policies to support the mission, goals, and priorities of the agency.

Chief Information Security Officer (CISO)

1. The CISO is the senior agency official responsible for the agency's Computer Security Program.
2. The CISO provides leadership input and oversight for all risk management and IT security activities across the agency.

3. The CISO functions as the NRC risk executive and identifies the overall risk posture based on the aggregated risk from each of the information systems and supporting infrastructures for which the organization is responsible (e.g., security categorizations, common security control identification). This helps ensure consistent risk acceptance decisions.

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, Formerly Restricted Data, and National Security Information 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 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 its classified status when in document form.
2. Classified information includes the following:
   (a) Restricted Data,
   (b) Formerly Restricted Data, and
   (c) National Security Information 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.

Clearing

1. The removal of data from a system, its storage devices, and other peripheral devices with storage capacity in a way that prevents the data from being reconstructed using common system capabilities (i.e., keyboard strokes); however, this data may be reconstructed using laboratory methods.
2. Cleared media may be reused at the same classification level or at a higher level.
3. Overwriting is one method of clearing.
4. See Magnetic Remanence.

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. 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.

Compartmentalization (Computer)

1. The isolation of the operating system, user programs, information, and data files from one another in main storage in order to provide protection against unauthorized or concurrent access by other users or programs.
2. The breaking down of sensitive data into small, isolated blocks for the purpose of reducing risk to the data.

Compilation

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

Compromise

The disclosure of classified information or administratively controlled information to persons not authorized to receive this information.

Compromising Emanations

1. The emanations of unintentional intelligence-bearing signals that if intercepted and analyzed disclose classified information being transmitted, received, handled, or otherwise processed by any information-processing system.
2. See also TEMPEST.

Computer Application

The use of information resources (information and information technology) to satisfy a specific set of user requirements.

Computer Center

1. One or more computers with their peripheral and storage units, central processing units, and communications equipment in a single controlled area.
2. The term “computer center” may also be referred to as an IT facility, an IT installation, an IT center, or an IT installation/center.

Computer Equipment

1. All forms of computers, personal digital assistants, mobile phones, smart cards, thumb drives, flash drives; and
2. Any other equipment used for storing, processing, or transmitting electronic information.

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 IT operation.

Computer Security

1. The protection of sensitive electronic information 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.

Computer Testing Tools

Tools used to determine if computer hardware, software, or firmware is operating as intended.

Computing Resources

Computing Resources include the following:

1. Computers and IT resources, including desktop and laptop computers, networks, facilities, printers, scanners, faxes, personal electronic devices (PEDs), electronic media, and printouts.
2. Any other IT used to store or process electronic information.
3. 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 COMSEC material.

COMSEC Accounting

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

COMSEC Control Officer

The individual designated by the supervisor of a secure communications facility to be in charge of the day-to-day operations of the facility.

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. COMSEC equipment includes the following:
   (a) Cryptoequipment,
   (b) Cryptoancillary equipment,

(c) Cryptoproduction equipment, and

(d) Authentication equipment.

COMSEC Facility

Authorized and approved space used for generating, storing, repairing, or using COMSEC material.

COMSEC Information

All information concerning COMSEC and all COMSEC material.

COMSEC Insecurity

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

COMSEC Manager

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

COMSEC Material

1. 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 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 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 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. COMSEC accounting,
2. Use of COMSEC aids, or
3. Use, maintenance, and repair of COMSEC equipment.

CONFIDENTIAL

"Confidential" is 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.

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.

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.

Configuration Management

The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of a system.

Contingency Plans

1. Plans for interim measures to continue operations after a disruption.
2. 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.

Contracting Officials

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

Controlled Area

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)

1. Secure telecommunications or information handling equipment, or an associated cryptographic component, that is unclassified but governed by a special set of control requirements.
2. These items are marked “CONTROLLED CRYPTOGRAPHIC ITEM” or, where space is limited, “CCI.”

Controlled Unclassified Information (CUI)

A new category of unclassified information that replaced the various categories used Governmentwide for sensitive but unclassified information. CUI was created by former President George W. Bush in a memorandum dated May 2008. In November 2010, an Executive order was issued by President Barack Obama that allowed for new handling of CUI to be established by the National Archives and Records Administration (NARA).

Control Zone

1. The space, expressed in feet of radius, surrounding equipment that meets the following requirements:
   (a) The equipment is used to process sensitive information, 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. 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.
2. 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. The importance of an asset or system to an organization.
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.

Cryptanalysis

1. The steps and operations performed in converting encrypted messages into plain text without the initial knowledge of the key employed in the encryption.
2. In 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

A marking or designator identifying all COMSEC keying material used to protect or authenticate telecommunications containing National Security Information and National Security-Related Information.

Cryptoequipment

Any equipment employing a cryptographic logic.

Cryptographic

Pertaining to or concerned with cryptography.

Cryptographic System

See Cryptosystem.

Cryptography

1. The use of mathematical manipulations to enable information confidentiality, integrity, authentication, authorization, and non-repudiation; and
2. The means and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

Cryptoinformation

Information that would make a significant contribution to the cryptoanalytic solution of encrypted text found in a cryptosystem.

Cryptoinsecurity

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

Cryptology

The field that encompasses both cryptography and cryptanalysis.

Cryptomaterial

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

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

Cryptoperiod

Time span during which each key setting remains in effect.

Cryptosecurity

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

Cryptosystem

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

Cryptovariable

See Keying Material.

Custodian

A person who possesses classified information or is otherwise charged with the responsibility to protect classified information.

Daemon

A computer process that runs in the background based upon a trigger event rather than under the direct control of a user.

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-Dependent Protection

Protection of data at a level commensurate with the sensitivity level of the individual data elements, rather than with the sensitivity of the entire file that includes the data elements.

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 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 apply a variable alternating current (AC) field for the purpose of demagnetizing magnetic recording media, usually tapes or disks.
2. The process that involves increasing the AC field gradually from zero to some maximum value and decreasing the field back to zero, leaving a very low residue of magnetic induction on the media.

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 to derivatively classify National Security Information, Restricted Data, and Formerly Restricted Data.
2. See also Derivative Classification and Authorized Classifier.

Designated Approving Authority (DAA)

1. The senior management official(s) with the authority to accept the adequacy of the security protection prescribed for IT systems.
2. The DAA is responsible for issuing an authorization decision to accept security protections based on a reasonable assessment of the risks and how effectively the protections mitigate the risks. Thus, the DAA accepts the risks associated with system operation.
3. At the NRC, the DAA is a committee comprised of the Deputy Executive Director for Corporate Management/CIO; the Deputy Executive Director for Materials, Waste, Research, State, Tribal and Compliance Programs; and the Deputy Executive Director for Reactor and Preparedness Programs.

Digital Signature

1. 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.
2. Besides being easily transportable, the digital signature ensures that the content of the message or document is unchanged.
3. When a message is time-stamped, it ensures that its sender cannot easily repudiate it later.
4. 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.

5. 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

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.

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, iPods, and MP3 players.

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 (i.e., both internal and external) and removable drives (e.g., external hard drives),
   (b) CDs,
   (c) Digital 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,
3. Access to Safeguards Information (SGI), or
4. Access to sensitive NRC automated information systems and data.

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 which 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 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 he or she 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. A comprehensive framework used to manage and align an organization's IT assets, people, operations, and projects with its operational characteristics.
2. The EA defines how information and technology will support the business operations and provide benefit for the business.
3. The EA illustrates the organization's core mission, each component critical to performing that mission, and how each of these components is interrelated.

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 13526

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

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[1]
2. A determination by the NRC that a facility may be used for electronic processing of NRC sensitive unclassified information.

Facility Register

An index of security facilities.

[1] Note: Only reactor design vendors are required to obtain the NRC's approval for a specific facility to handle safeguards information related to aircraft impact analysis.

Foreign 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, typically 6 months or more.

Foreign Government Information

1. Information provided to the U.S. Government that meets the following criteria:
   (a) The information is provided by—
      (i) A foreign government or governments, or
      (ii) An international organization of governments or any element thereof.
   (b) The information is provided with the expectation that the information, the source of the information, or both are to be held in confidence.
2. Information produced by the U.S. Government that meets the following general criteria:
   (a) The information is created or shared pursuant to or the result of a joint arrangement with one of the following:
      (i) A foreign government or governments, or
      (ii) An international organization of governments or any element thereof.
   (b) The information or the arrangement between the U.S. Government and the other parties is to be held in confidence.
3. Information received and treated as “foreign government information” under the terms of an applicable Executive order.

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. 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, 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 would 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 MD 12.3, “NRC Personnel Security Program.”

Hearing Examiner

A qualified attorney appointed by the Director of the Office of Administration 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 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 computer that provides services to other computers or to users.

Identification, User

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).

Identification and Authentication (I&A)

The combination of the two processes described below.

1. Identification

   Process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.

2. Authentication

   The 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.

Illegal Alien

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

Immigrant Alien

An alien who has been granted the right by the United States Citizenship and Immigration Services (USCIS) to reside permanently in the United States and to work without restrictions in the United States.

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 SGI 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

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 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. The organizational official with statutory or operational authority for specified information who is responsible for establishing the policies and procedures governing 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 Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

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 cyber security controls are in place, operating as intended, and having the desired effect for a system, program, or enclave.

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 Resources

1. Includes, but is not limited to, hardware, application software, system software, and information (data).
2. 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 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 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.

Infraction

A failure to comply with NRC security requirements or procedures that does not constitute a violation of law.

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 of 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, as amended, 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, as amended, and/or applicable statute.

Intelligence Community Member

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) Air Force Intelligence,
   (b) Army Intelligence,
   (c) Central Intelligence Agency,
   (d) Coast Guard Intelligence;
   (e) Defense Intelligence Agency,
   (f) Department of Energy,
   (g) Department of Homeland Security,
   (h) Department of State,
   (i) Department of the Treasury,
   (j) Drug Enforcement Administration,
   (k) Federal Bureau of Investigation,
   (l) Marine Corps Intelligence,
   (m) National Geospatial-Intelligence Agency,
   (n) National Reconnaissance Office,
   (o) National Security Agency, and
   (p) Navy Intelligence.

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.

Interim Access Authorization

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

Internal Security Audit

1. A security audit conducted by personnel responsible to the management of the organization being audited.
2. The term Internal Security Audit in this context is related to Information Technology.

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)

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.

Inventory Report, COMSEC

A report submitted to the National Security Agency COR with a copy to the NRC agency COMSEC custodian (NRC COR) attesting to the inventory of accountable COMSEC material.

Inventory, COMSEC

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

IT Coordinator

1. The individual appointed by the office director/regional administrator to serve as liaison between each NRC office and the Office of Information Services (OIS) regarding 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 OIS,
   (b) Attend OIS briefings on IT issues,
   (c) Serve as office liaison between office staff and the OIS to coordinate agencywide software upgrades,
   (d) Inform the OIS 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 Sensitive Unclassified Non-safeguards Information (SUNSI).

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.

IT Media

1. Any storage device that holds digital data and is not considered an 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 cryptovariables for machine cryptosystems.

Keyword

Synonym for “Password.”

“L” Access Authorization

1. An “L” access authorization is normally based upon an ANACI conducted by the Office of Personnel Management.
2. This authorization permits individuals access, on a need-to-know basis, to SECRET and CONFIDENTIAL National Security Information or CONFIDENTIAL RD not related to broad naval nuclear propulsion program policy or direction.

Least Privilege

1. The principle that requires that each subject (i.e., user or process) be granted the most restrictive set of privileges needed for the performance of authorized tasks.

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 unclassified official information originated by the Department of State in oral or documentary form, which 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)

An interconnected group of office automation systems or system components that is physically located within a small physical area, such as a building or a campus.

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.

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 physical act of indicating on a classified document the assigned classification, changes in classification, downgrading and declassification instructions, and any limitations on its use.

2. The physical act of indicating on a sensitive unclassified information document the assigned category, changes in the sensitive unclassified information category, and removal from the sensitive unclassified information category.
3. The physical act of indicating on an unclassified document that it contains unclassified information.

Master Facility Register

A central index maintained by the Division of Facilities and Security 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.

Monitor Sheet

A printed security form, generally placed next to a security container, vault, vault-type room, or secure telephone, that is initialled on a scheduled basis by the person(s) assigned to monitor the security of the unit.

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 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 sensitive information, be it National Security Information, Safeguards Information, or SUNSI, that a proposed recipient's access to the sensitive information is necessary in the performance of an official and lawful requirement.

2. A need-to-know determination must also be conducted for a prospective recipient to gain access to Safeguards Information and sensitive unclassified information.

Network

A system of two or more computers that can exchange data or information.

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 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 an other classification authority.

Original Classifier

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

Page Check

A check of the pages contained within an item of accountable 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 CD, DVD, and 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. P2P is used primarily for ad hoc or unplanned connections between the participating computers and their users.

Personal Digital Assistant (PDA)

A small, mobile, lightweight, hand-held computer or electronic device designed for use as a personal organizer with communications capabilities.

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. PII is a person's name, in combination with any of the following information:
   (a) Relatives' names,
   (b) Postal address,
   (c) E-mail 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 e-mail 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 e-mail address.

Personnel Security

The procedures established to ensure that all personnel who have access to sensitive information have met all investigative requirements and have been granted appropriate clearances.

Physical Security

The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.

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)

Examples of PEDs include PDA (e.g., Palm Pilot), cell phone, smart phone, text messaging systems (e.g., BlackBerry), universal serial bus (USB) flash memory (e.g., thumb drive), external drive, and plug-in and wireless peripheral.

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 person with either limited or unlimited privileged access to a computing resource, such as a system administrator or information system security officer.
2. A privileged user may use and access privileged information on all or part of the computing resource.
3. 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,

   (b) 10 CFR 2.336,

   (c) 10 CFR 2.390,

   (d) 10 CFR Part 9 (Section 9.17), and

   (e) 10 CFR Part 52.

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 Sensitive Unclassified Non-Safeguards Information.

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)

A method of providing high-level encryption, authentication, and digital signature capability based on public key certificates.

Purging

Rendering stored information unrecoverable. (See Sanitizing.)

"Q" Access Authorization

1. A "Q" access authorization is normally based upon a single-scope, full-field background investigation (SSBI) conducted by the Office of Personnel Management 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.

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 (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)).

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.

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

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. RD does not include data declassified or removed from the RD category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended.

Risk

1. The probability that a particular threat will adversely impact an information system by exploiting a particular vulnerability.
2. 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.
3. 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 man-made disasters; and
   (d) Failure to exercise due care and diligence in the implementation and operation of the IT system.

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 agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.
2. Part of risk management, synonymous with Risk Analysis, and incorporates threat and vulnerability analyses.

Risk Evaluations

The process of comparing the estimated risks against risk criteria to determine the significance of the risks.

Risk Management

1. The process of identifying, controlling, and mitigating risks related to information systems.
2. It includes risk assessment, cost-benefit analysis, and the selection, implementation, testing, and evaluation of security protections.
3. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.

Safeguarding

Measures and controls that are prescribed to protect classified information.

Safeguards Information (SGI)

1. Sensitive unclassified information that specifically identifies the detailed security measures of a 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. 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.

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

1. The SLES 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. SGI LAN provides secure wireless access to E-Safe.
4. E-Safe is the agency's official record keeping system for SGI.

Safeguards Information - Modified Handling (SGI-M)

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.

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.

SBU

See Sensitive But Unclassified.

Scavenging

Searching through residue for the purpose of data acquisition.

SCI

See Sensitive Compartmented Information.

SECRET

"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.

Secret Internet Protocol Router Network (SIPRNet)

1. 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) via 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 SCI Joint Worldwide Intelligence Communications System.
4. The DOD Non-Classified Internet Protocol Router Network (NIPRNet) is used to control 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.

Security Area

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

Security Assessment

1. 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.
2. The term Security Assessment in this context is related to Information Technology.

Security Assurance

A written certification by which an authorized official of a foreign government or an international organization with which the United States has an international agreement covering the exchange of classified information informs the U.S. Government of the category of a security clearance held by a foreign national, the scope of the investigation upon which the clearance determination is based, and personal identity data.

Security Clearance

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

Security Control Assessor (Formerly Certification Authority)

Official responsible for performing the comprehensive evaluation of the security features of an information system and determining the degree to which the features meet security requirements.

Security Controls

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.

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.

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.

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., a telecommunications or an information technology 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, sensitive unclassified information, or both; and
   (c) Protect personnel and property.

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 But Unclassified (SBU)

Information that is not classified for national security reasons, but that warrants/requires administrative control and protection from public or other unauthorized disclosure for other reasons. SBU should meet one or more of the criteria for exemption from public disclosure under the Freedom of Information Act (FOIA) (which also exempts information protected under other statutes) (5 U.S.C. 552), or should be protected by the Privacy Act (5 U.S.C. 552a).

Sensitive Compartmented Information (SCI)

1. All information and materials requiring special community controls indicating restricted handling within present and future community intelligence collection programs and their end products.
2. These special community controls are formal systems of sources and methods and analytical procedures of foreign intelligence programs.
3. The term does not include Restricted Data 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 SCI may be stored, used, discussed, or processed.

Sensitive Information

1. A generic term used to identify information designated as classified information, SGI, or SUNSI.
2. Sensitive information includes any information or material, regardless of its physical form or characteristics, which meets the following two requirements:
   (a) The information or material is originated, owned, or possessed by the United States Government; and
   (b) A compromise of the confidentiality, integrity, or availability of the information could have an adverse effect on government operations, government assets, or individuals.

Sensitive System

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

Sensitive Unclassified Non-safeguards Information (SUNSI)

Any information that, if lost, misused, modified, or accessed without authorization could reasonably be foreseen to harm one or more of the following:

1. The public interest,
2. The commercial or financial interests of the entity or individual to whom the information pertains,
3. The conduct of NRC and Federal programs, or
4. The personal privacy of individuals.

Sensitivity Level

Sensitivity Level is 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 work stations share common facilities.

Shared Logic Word Processing Equipment

Word processing equipment in which the resources for a processing unit and storage devices are shared between two or more work stations.

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 for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information 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 SGI or classified information on the NRC LAN/WAN or a device not approved for SGI 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, for example, 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.

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. 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 or not any deliberate attempt by personnel or failure of system components could adversely affect the common defense and security.

System Security Plan (SSP)

1. Formal document that accomplishes the following:
   (a) Provides an overview of the security requirements for the information system, and
   (b) Describes the security controls that are/will be in place for meeting those requirements.
2. The SSP ensures that the security controls of the system can be reconstructed.

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 preparation, transmission, communication, or processing of information by electrical, electromagnetic, electromechanical, or electro-optical means.

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 sensitive 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.

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 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

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.)

Traffic

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

Transaction

1. 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.
2. A transaction has to be completed in its entirety for a transaction to be completed and database changes to made permanent.
3. The term “transaction” in this context is related to Information Technology.

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 IT Security, Data Security, Communications Security, and Teleprocessing Security.

Trojan Horse

1. A computer program containing the following:

   (a) Apparent or actual useful function, and

(b) Additional functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security.

2. For example, such a computer program might make a “blind copy” of a sensitive file.
3. See Malicious Code.

Trusted Agent

1. Entity authorized to act as a representative of an organization in confirming subscriber identification during the registration process.
2. Trusted agents do not have automated interfaces with certification authorities.

TSCM

See Technical Surveillance Countermeasures.

Unauthorized Disclosure

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

Unclassified System

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

Upgrade

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 alien 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 who owes his sole allegiance to the United States, including all U.S. citizens, and including some individuals who are not U.S. citizens. For tax purposes, the term "U.S. national" refers to 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

The performance of tests and evaluations in order to determine compliance with security specifications and 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 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. Self-replicating, malicious code that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence.
2. The term Virus in this context is related to the term Information Technology.

Vulnerability

1. A weakness in system security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.
2. The term Vulnerability in this context is related to the term Information Technology.

Vulnerability Assessment

The systematic examination of telecommunications to accomplish the following:

1. Determine the adequacy of COMSEC measures,
2. Identify COMSEC deficiencies,
3. Provide data from which to predict the effectiveness of proposed COMSEC measures, and
4. 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 network that provides data communication capabilities in geographic areas larger than those served by LANs.

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 cryptovariable distributed by a key generation facility for use on a specific interstation call.

III. REFERENCES

Code of Federal Regulations

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 73, "Physical Protection of Plants and Materials."

Executive Orders

E.O. 12333, as amended, "United States Intelligence Activities," December 4, 1981.

E.O. 12968, "Access to Classified Information," August 2, 1995.

E.O. 13526, "Classified National Security Information," December 29, 2009.

E.O. 13556. "Controlled Unclassified Information," November 4, 2010.

National Security Council Documents

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

Nuclear Regulatory Commission Documents

Management Directive—

12.1, "NRC Facility Security Program."

12.2, "NRC Classified Information Security Program."

12.3, "NRC Personnel Security Program."

12.4, "NRC Telecommunications Systems Security Program."

12.5, "NRC Cyber Security Program."

12.6, "NRC Sensitive Unclassified Information Security Program."

12.7, "NRC Safeguards Information Security Program."

Yellow Announcement YA-05-0077, "Policy Revision: NRC Policy and Procedures for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information (SUNSI)," October 26, 2005 (ADAMS Accession No. ML051220278).

United States Code

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

Computer Security Act of 1987 (15 U.S.C. Sec. 278).

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 USC 3504 et. seq.).

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