Committee on National Security Systems

CNSSI No. 4009
April 6, 2015

Committee on National Security Systems (CNSS) Glossary

THIS DOCUMENT PRESCRIBES MINIMUM STANDARDS
YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER
IMPLEMENTATION

National Manager

FOREWORD

1. The Committee on National Security Systems (CNSS) Glossary Working Group convened to review and update the Committee on National Security Systems (CNSS) Glossary, Committee on National Security Systems Instruction (CNSSI) No. 4009, dated April 2010. This revision of CNSSI No. 4009 incorporates many new terms submitted by the CNSS Membership. Most of the terms from the 2010 version of the Glossary remain, but a number of terms have updated definitions in order to remove inconsistencies among the communities.

2. The Glossary Working Group set several overall objectives for itself in producing this version:

- Use authoritative sources for definitions of terms. It is preferred that definitions originate from current authoritative sources, as this demonstrates both that the term is in active use and that the definition has been vetted by subject matter experts. Listing sources for terms also provides context and a reference for additional information. The glossary still contains terms where sources are not specified. For these terms, definitions will be considered organic. The majority of unsourced terms are from the CNSSI No. 4009 (2010) version, although some are newly introduced. These new terms are primarily emerging terms judged to be valuable to include in the glossary, but for whatever reason have not yet been defined in a published authoritative source.
- Continue to resolve differences between the definitions of terms used by the Department of Defense (DoD), Intelligence Community (IC), and Civil Agencies (e.g. National Institute of Standards and Technology (NIST)); enabling all three to use the same glossary. This will allow for use of consistent terminology in documentation, policy, and process across these communities.
- Ensure consistency among related and dependent terms. These terms are linked through a suggestion to see the related term.
- Ensure any acronyms used in the terms and definitions also appear in the Acronyms appendix, and remove any acronyms judged to be outside of the scope of the glossary or no longer relevant.
- Ensure all documents referenced as sources in the terms and definitions also appear in the References appendix. Because of this, the number of references has grown from 29 in the 2010 version to over 150 in the current version. References not used as the source of terms and definitions were removed.

3. Many cyber terms are emerging. The Glossary Working Group has tried to include significant terms and definitions that have a useful distinction when compared to existing Information Assurance terms. All terms currently defined in CNSS issuances were reviewed for either inclusion or to replace current definitions in the Glossary. Not all terms appearing in CNSS issuances are within the scope of the CNSS Glossary or are relevant to a broad audience.

4. Some terms and definitions recommended by the community for inclusion were not

added to this version of the glossary. The main reasons for not adding new terms or definitions were ones of scope or lack of an authoritative source, where an organic definition was not deemed appropriate.

5. Many terms that are outdated or no longer necessary were removed from the glossary. Some of these had been labeled as Candidates for Deletion (C.F.D.) for several versions of the glossary, but continue to remain in this version. A term labeled "C.F.D." may be obsolete; however without the term, rationale and possible linkage to a new term, users of the glossary would have no indication the term is outdated or has been replaced by a new term.

6. We recognize an effective glossary must be in a continuous state of coordination and improvement. We encourage further community review and comments as new terms become significant and old terms fall into disuse or change meaning. The goal of the Glossary Working Group is to keep the CNSS Glossary relevant and a tool for commonality across the IA community.

7. Representatives of the CNSS may obtain copies of this instruction on the CNSS Web Page at http://www.cnss.gov.

FOR THE NATIONAL MANAGER:

/s/

CURTIS W. DUKES

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

National Information Assurance (IA) Glossary

Terms and Definitions

This instruction applies to all U.S. Government Departments, Agencies, Bureaus and Offices; supporting contractors and agents; that collect, generate process, store, display, transmit or receive classified or controlled unclassified information or that operate, use, or connect to National Security Systems (NSS), as defined herein.

Term **Definition**

access

Ability to make use of any information system (IS) resource.

Source: NIST SP 800-32

access authority

An entity responsible for monitoring and granting access privileges for other authorized entities.

access control

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

Source: FIPS PUB 201-1 (adapted)

access control list (ACL)

A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.

access control mechanism

Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system.

access cross domain solution

A type of cross domain solution (CDS) that provides access to a computing platform, application, or data residing on different security domains from a single device.

Source: CNSSI No. 1253F Attachment 3

access level

A category within a given security classification limiting entry or system connectivity to only authorized persons.

access list

Roster of individuals authorized admittance to a controlled area.

access profile

Association of a user with a list of protected objects the user may access.

access type

Privilege to perform action on an object. Read, write, execute, append, modify, delete, and create are examples of access types.

accountability

1. The principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

2. The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

Source: NIST SP 800-27 Rev A

accounting legend code (ALC)

A numeric code used to indicate the minimum accounting controls required for items of accountable COMSEC material within the COMSEC material control system (CMCS).

Source: NSA/CSS Manual Number 3-16 (COMSEC)

accounting number

A number assigned to an individual item of COMSEC material to facilitate its handling and accounting.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

accreditation (C.F.D.)

Formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

See authorization to operate (ATO).

Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called authorization.

accreditation boundary (C.F.D.)

1. Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged via messaging. Synonymous with Security Perimeter.

2. For the purposes of identifying the Protection Level for confidentiality of a system to be accredited, the system has a conceptual boundary that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system. See authorization boundary.

Rationale: The Risk Management Framework uses a new term to refer to the concept of accreditation, and it is called authorization. Extrapolating, the accreditation boundary would then be referred to as the authorization boundary.

accreditation package (C.F.D.)

Product comprised of a system security plan (SSP) and a report documenting the basis for the accreditation decision.

Rationale: The RMF uses a new term to refer to this concept, and it is called RMF security authorization package.

accrediting authority (C.F.D.)

Synonymous with designated accrediting authority (DAA). See also authorizing official.

Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called authorizing official (AO).

acquirer

Stakeholder that acquires or procures a product or service.

Source: NIST IR 7622, ISO/IEC 15288 (adapted)

activation data

A pass-phrase, personal identification number (PIN), biometric data, or other mechanisms of equivalent authentication robustness used to protect access to any use of a private key, except for private keys associated with System or Device certificates.

Source: CNSSI No. 1300

active attack

An attack on the authentication protocol where the Attacker transmits data to the Claimant, Credential Service Provider, Verifier, or Relaying Party. Examples of active attacks include man-in-the middle, impersonation, and session hijacking.

Source: NIST SP 800-63-2

active content

Electronic documents that can carry out or trigger actions automatically on a computer platform without the intervention of a user.

Source: NIST SP 800-28

active cyber defense

Synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities.

Source: DSOC 2011

activities (assessment)

An assessment object that includes specific protection related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic).

Source: NIST SP 800-53A Rev 1

add-on security (C.F.D.)

Incorporation of new or additional hardware, software, or firmware safeguards in an operational information system.

adequate security

Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Source: OMB Circular A-130

administrative incident (COMSEC)

A violation of procedures or practices dangerous to security that is not serious enough to jeopardize the integrity of a controlled cryptographic item (CCI), but requires corrective action to ensure the violation does not recur or possibly lead to a reportable COMSEC incident.

Source: CNSSI No. 4001 (adapted)

advanced encryption standard (AES)

A U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

Source: FIPS PUB 197 (adapted)

advanced key processor (AKP)

A cryptographic device that performs all cryptographic functions for a management client node and contains the interfaces to 1) exchange information with a client platform, 2) interact with fill devices, and 3) connect a client platform securely to the primary services node (PRSN).

advanced persistent threat (APT)

An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.

Source: NIST SP 800-39

adversary

Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Source: NIST SP 800-30 Rev 1

advisory (C.F.D.)

Notification of significant new trends or developments regarding the threat to the information systems of an organization. This notification may include analytical insights into trends, intentions, technologies, or tactics of an adversary targeting information systems.

Rationale: General definition of a commonly understood term.

agency

Any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the government (including the Executive Office of the President), or any independent regulatory agency, but does not include -
(i) the General Accounting Office;
(ii) Federal Election Commission;
(iii) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or
(iv) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities.
See also executive agency.

Source: 44 U.S.C., Sec. 3502

air gap

An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control).

Source: IETF RFC 4949 Ver 2

alert

Notification that a specific attack has been directed at an organization's information systems.

allied nation

A nation allied with the U.S. in a current defense effort and with which the U.S. has certain treaties. For an authoritative list of allied nations, contact the Office of the Assistant Legal Adviser for Treaty Affairs, Office of the Legal Adviser, U.S. Department of State, or see the list of U.S. Collective Defense Arrangements at www.state.gov.

Source: CNSSI No. 4005 (COMSEC)

allocation

The process an organization employs to determine whether security controls are defined as system-specific, hybrid, or common.

The process an organization employs to assign security controls to specific information system components responsible for providing a particular security capability (e.g., router, server, remote sensor).

Source: NIST SP 800-37 Rev 1

all-source intelligence

Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data in the production of finished intelligence.

Source: DoD JP 1-02 (adapted); NIST SP 800-53 Rev 4 (adapted)

alternate COMSEC account manager

The primary alternate COMSEC Account Manager is an individual designated by proper authority to perform the duties of the COMSEC Account Manager during the temporary authorized absence of the COMSEC Account Manager. Additional alternate COMSEC Account Managers may be appointed, as necessary, to assist the COMSEC Account Manager and maintain continuity of operations.

Source: CNSSI No. 4005 (COMSEC)

alternate COMSEC custodian (C.F.D.)

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

Source: NSA/CSS Manual Number 3-16 (COMSEC)

analysis approach

The approach used to define the orientation or starting point of the risk assessment, the level of detail in the assessment, and how risks due to similar threat scenarios are treated.

Source: NIST SP 800-30 Rev 1

anti-jam

The result of measures to resist attempts to interfere with communications reception.

Source: CNSSI No. 1200

anti-signal fingerprint

Result of measures used to resist attempts to uniquely identify a particular transmitter based on its signal parameters.

Source: CNSSI No. 1200

anti-signal spoof

Result of measures used to resist attempts to achieve imitative or manipulative communications deception based on signal parameters.

Source: CNSSI No. 1200

anti-spoof

Countermeasures taken to prevent the unauthorized use of legitimate identification & authentication (I&A) data, however it was obtained, to mimic a subject different from the attacker.

anti-tamper (AT)

Systems engineering activities intended to deter and/or delay exploitation of critical technologies in a U.S. defense system in order to impede countermeasure development, unintended technology transfer, or alteration of a system.

See tampering.

Source: DoDI 5200.39

application

A software program hosted by an information system.

Source: NIST SP 800-37 Rev 1

application-specific integrated circuits (ASICs)

Custom-designed and/or custom-manufactured integrated circuits.

Source: CNSSD No. 505

approval to operate (ATO) (C.F.D.)

The official management decision issued by a designated accrediting authority (DAA) or principal accrediting authority (PAA) to authorize operation of an information system and to explicitly accept the residual risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. See authorization to operate (ATO).

Rationale: Term has been replaced by the term “authorization to operate (ATO)”.

assembly

An item forming a portion of an equipment, that can be provisioned and replaced as an entity and which normally incorporates replaceable parts and groups of parts.

Source: DoD 4140.1-R; CNSSI No. 4033

assessment

See security control assessment or risk assessment.

Source: NIST SP 800-30 Rev 1

assessment approach

The approach used to assess risk and its contributing risk factors, including quantitatively, qualitatively, or semi-quantitatively.

Source: NIST SP 800-30 Rev 1

assessment findings

Assessment results produced by the application of an assessment procedure to a security control or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a satisfied or other than satisfied condition.

Source: NIST SP 800-53A Rev 1

assessment method

One of three types of actions (i.e., examine, interview, test) taken by assessors in obtaining evidence during an assessment.

Source: NIST SP 800-53A Rev 1

assessment object

The item (i.e., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.

Source: NIST SP 800-53A Rev 1

assessment objective

A set of determination statements that expresses the desired outcome for the assessment of a security control or control enhancement.

Source: NIST SP 800-53A Rev 1

assessment procedure

A set of assessment objectives and an associated set of assessment methods and assessment objects.

Source: NIST SP 800-53A Rev 1

assessor

See security control assessor or risk assessor.

Source: NIST SP 800-30 Rev 1

asset

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

asset reporting format

A format for expressing the transport format of information about assets and the relationships between assets and reports.

Source: NIST SP 800-126 Rev 2

assurance

The grounds for confidence that the set of intended security controls in an information system are effective in their application.

Source: NIST SP 800-27 Rev A (adapted)

assurance case

A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute.

Source: NIST SP 800-39; NIST SP 800-53 Rev 4

assured information sharing

The ability to confidently share information with those who need it, when and where they need it, as determined by operational need and an acceptable level of security risk.

assured software

Computer application that has been designed, developed, analyzed and tested using processes, tools, and techniques that establish a level of confidence in it.

asymmetric cryptography

See public key cryptography (PKC).

asymmetric key

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.

Source: FIPS PUB 201-1; NIST IR 7298 Rev 2 attack

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

attack sensing and warning
(AS&W)

Detection, correlation, identification, and characterization of intentional unauthorized activity with notification to decision makers so that an appropriate response can be developed.

attack signature

A specific sequence of events indicative of an unauthorized access attempt.

Source: NIST SP 800-12

attack tree

A branching, hierarchical data structure that represents a set of potential approaches to achieving an event in which system security is penetrated or compromised in a specified way.

Source: IETF RFC 4949 Ver 2

attended

Under continuous positive control of personnel authorized for access or use.

Source: CNSSI No. 4005 (COMSEC); NSA/CSS Manual Number 3-16 (COMSEC)

attribute

An attribute is any distinctive feature, characteristic, or property of an object that can be identified or isolated quantitatively or qualitatively by either human or automated means.
Source: ISO/IEC 27000

attribute-based access control (ABAC)

Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place.

See also identity, credential, and access management (ICAM).

attribute-based authorization

A structured process that determines when a user is authorized to access information, systems, or services based on attributes of the user and of the information, system, or service.

audit

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

audit log

A chronological record of system activities. Includes records of system accesses and operations performed in a given period.

audit record

An individual entry in an audit log related to an audited event.

Source: NIST SP 800-53 Rev 4

audit reduction tools

Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance.

Source: NIST SP 800-12

audit trail

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

2. A record showing who has accessed an information technology (IT) system and what operations the user has performed during a given period.

Source: NIST SP 800-47

authenticate

To confirm the identity of an entity when that identity is presented.

Source: NIST SP 800-32

authentication

1. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Source: FIPS PUB 200; NIST SP 800-27 Rev A

2. A security measure designed to protect a communications system against acceptance of fraudulent transmission or simulation by establishing the validity of a transmission, message, originator, or a means of verifying an individual's eligibility to receive specific categories of information.

Source: CNSSI No. 4005 (COMSEC); NSA/CSS Manual Number 3-16 (COMSEC)

authentication mechanism

Hardware or software-based mechanisms that force users to prove their identity before accessing data on a device.

Source: NIST SP 800-72

authentication period

The period between any initial authentication process and subsequent re-authentication processes during a single terminal session or during the period data is being accessed.

authentication protocol

1. A well specified message exchange process between a claimant and a verifier that enables the verifier to confirm the claimant's identity.

2. A defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has possession and control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier.

Source: NIST SP 800-63-2

authenticator

The means used to confirm the identity of a user, process, or device (e.g., user password or token).

Source: NIST SP 800-53 Rev 4

authenticity

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.

Source: NIST SP 800-53 Rev 4; NIST SP 800-53A Rev 1; NIST SP 800-39 authority (C.F.D.)

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

Rationale: General definition of a commonly understood term.

authorization

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

authorization boundary

All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

Source: NIST SP 800-53 Rev 4; NIST SP 800-53A Rev 1; NIST SP 800-37 Rev 1

authorization package

See security authorization package

authorization to operate (ATO)

The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Source: NIST SP 800-53 Rev 4; NIST SP 800-53A Rev 1; NIST SP 800-37 Rev 1

authorize processing

See authorization.

Source: NIST SP 800-53 Rev 4; NIST SP 800-37 Rev 1

authorized ID

The key management entity (KME) authorized to order against a traditional short title.

Source: CNSSI No. 4005 (COMSEC)

authorized user

Any appropriately cleared individual with a requirement to access an information system (IS) for performing or assisting in a lawful government purpose.

Source: DoDD 8570.01 (adapted)

authorized vendor

Manufacturer of information security (INFOSEC) equipment authorized to produce quantities in excess of contractual requirements for direct sale to eligible buyers. Eligible buyers are typically U.S. Government organizations or U.S. Government contractors.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

authorizing official

A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Source: NIST SP 800-37 Rev 1; NIST SP 800-53 Rev 4

authorizing official designated representative

An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.

Source: NIST SP 800-37 Rev 1; DoDI 8510

automated security monitoring

Use of automated procedures to ensure security controls are not circumvented or the use of these tools to track actions taken by subjects suspected of misusing the information system.

See information security continuous monitoring.

automatic remote rekeying

Procedure to rekey distant cryptographic equipment electronically without specific actions by the receiving terminal operator. See manual remote rekeying.

availability

1. Ensuring timely and reliable access to and use of information.

Source: 44 U.S.C. Sec 3542

2. Timely, reliable access to data and information services for authorized users.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

backdoor

An undocumented way of gaining access to computer system. A backdoor is a potential security risk.

Source: NIST SP 800-82 Rev 1

backup

A copy of files and programs made to facilitate recovery, if necessary.

Source: NIST SP 800-34 Rev 1

banner

Display on an information system that sets parameters for system or data use.

baseline

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

baseline configuration

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

Source: NIST SP 800-53 Rev 4

basic testing

A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as black box testing.

Source: NIST SP 800-53A Rev 1

bastion host

A special purpose computer on a network where the computer is specifically designed and configured to withstand attacks.

behavior analysis

The act of examining malware interactions within its operating environment including file systems, the registry (if on Windows), the network, as well as other processes and Operating System components.

Source: CNSSI No. 1011

benign environment

A non-hostile location protected from external hostile elements by physical, personnel, and procedural security countermeasures.

bi-directional (CDS) A cross domain device or system with the capability to provide both the transmission and reception of information or data between two or more different security domains (e.g., between TS/SCI and Secret or Secret and Unclassified).

binding Process of associating two related elements of information.

biometric 1. Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity of, an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics.

Source: FIPS PUB 201-1 (adapted)

2. A physical or behavioral characteristic of a human being.

Source: NIST SP 800-32

bit A binary digit having a value of 0 or 1.

Source: FIPS PUB 180-4

bit error rate Ratio between the number of bits incorrectly received and the total number of bits transmitted through a communications channel. Also applies to storage.

BLACK 1. Designation applied to encrypted information and the information systems, the associated areas, circuits, components, and equipment processing that information. See also RED.

Note: Includes BLACK data.

Source: CNSSI No. 4005 (COMSEC)

2. Designation applied to information systems, and to associated areas, circuits, components, and equipment, in which national security information is encrypted or is not processed.

Source: CNSSAM TEMPEST/01-13; NSTISSI No. 7002 (adapted)

black box testing See basic testing.

Source: NIST SP 800-53A Rev 1

black core A communication network architecture in which user data traversing a global internet protocol (IP) network is end-to-end encrypted at the IP layer. Related to striped core.

BLACK data Data that is protected by encryption so that it can be transported or stored without fear of compromise. Also known as encrypted data.

Source: CNSSI No. 4005 (COMSEC)

blacklist A list of discrete entities, such as hosts or applications that have been previously determined to be associated with malicious activity.

Also known as dirty word list.

Source: NIST SP 800-94

blacklisting

The process used to identify: (i) software programs that are not authorized to execute on an information system; or (ii) prohibited universal resource locators (URL)/websites.

Source: NIST SP 800-53 Rev 4

blended attack

A type of attack that combines multiple attack methods against one or more vulnerabilities.

Blue Team

1. The group responsible for defending an enterprise’s use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically the Blue Team and its supporters must defend against real or simulated attacks 1) over a significant period of time, 2) in a representative operational context (e.g., as part of an operational exercise), and 3) according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team).

2. A group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cybersecurity readiness posture. Often times a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems.

body of evidence (BoE)

The set of data that documents the information system’s adherence to the security controls applied.

boundary

Physical or logical perimeter of a system.

boundary protection

Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g. gateways, routers, firewalls, guards, encrypted tunnels).

Source: NIST SP 800-53 Rev 4

boundary protection device

A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.

Source: NIST SP 800-53 Rev 4

browsing

Act of searching through information system storage or active content to locate or acquire information, without necessarily knowing the existence or format of information being sought.

buffer overflow

A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.

Source: CNSSI No. 1011; NIST SP 800-28

bulk encryption

Simultaneous encryption of all channels of a multi-channel telecommunications link.

business continuity plan (BCP)

The documentation of a predetermined set of instructions or procedures that describe how an organization’s mission/business processes will be sustained during and after a significant disruption.

Source: NIST SP 800-34 Rev 1

business impact analysis (BIA)

An analysis of an information system’s requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Source: NIST SP 800-34 Rev 1

call back

Procedure for identifying and authenticating a remote information system terminal, whereby the host system disconnects the terminal and reestablishes contact.

canister (COMSEC) (C.F.D.)

Type of physical protective packaging used to contain and dispense keying material in punched or printed tape form.

Rationale: Although being phased out, canisters are still in circulation. However term is being marked C.F.D. in anticipation of removal in the future.

cascading (Cross Domain)

The downward flow of information through a range of security levels greater than the accreditation range of a system, network, or component without passing through an isolated device that implements the enforcement of all applicable approved policy decisions for each domain transfer.

Source: DoDI 8540.01

categorization

See security categorization.

Source: NIST SP 800-137

category (C.F.D.)

Restrictive label applied to classified or unclassified information to limit access.

central facility (or Tier 0)

See Tier 0.

Source: CNSSI No. 4032

central office of record (COR)

The entity that keeps records of accountable COMSEC material held by COMSEC accounts subject to its oversight.

Source: CNSSI No. 4005 (COMSEC)

central services node (CSN)

The Key Management Infrastructure core node that provides central security management and data management services.

certificate

A digitally signed representation of information that 1) identifies the authority issuing it, 2) identifies the subscriber, 3) identifies its valid operational period (date issued / expiration date). In the information assurance (IA) community, certificate usually implies public key certificate and can have the following types:

A digital representation of information which at least (1) identifies the certification authority (CA) issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.

Source: NIST SP 800-32; CNSSI No. 1300

See cross certificate, encryption certificate, and identity certificate.

certificate authority workstation (CAW)

The computer system or systems that process certification authority (CA) software and/or have access to the CA private keys, end entity keys, or end entity public keys prior to certification.

Source: NIST CP-1

certificate management

Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed.

certificate policy (CP)

1. A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Source: NIST SP 800-32

2. A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

Source: CNSSI No. 1300

certificate revocation list (CRL)

1. A list of revoked public key certificates created and digitally signed by a Certificate Authority.

Source: NIST SP 800-63-2; FIPS PUB 201-1

2. These are digitally signed "blacklists" of revoked certificates. Certification authorities (CAs) periodically issue certificate revocation lists (CRLs), and users can retrieve them on demand via repositories.

Source: CNSSI No. 1300

certificate status authority (CSA)

A trusted entity that provides on-line verification to a relying party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.

Source: NIST SP 800-32

certificate status server (CSS)

An authority that provides status information about certificates on behalf of the CA through online transactions (e.g., an online certificate status protocol (OCSP) responder).

Source: CNSSI No. 1300

certificate-related information

Information, such as subscriber's postal address, that is not included in a certificate. May be used by a certification authority (CA) managing certificates.

Source: NIST SP 800-32

certification

Comprehensive evaluation of an information system component that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

certification analyst (C.F.D.)

The independent technical liaison for all stakeholders involved in the certification and accreditation (C&A) process responsible for objectively and independently evaluating a system as part of the risk management process. Based on the security requirements documented in the security plan, performs a technical and non-technical review of potential vulnerabilities in the system and determines if the security controls (management, operational, and technical) are correctly implemented and effective.

certification authority (CA)

An entity authorized to create, sign, issue, and revoke public key certificates.

Source: CNSSI No. 1300 (adapted)

certification authority workstation (CAW) (C.F.D.)

Commercial-off-the-shelf (COTS) workstation with a trusted operating system and special purpose application software that is used to issue certificates.

Rationale: Term has been replaced by the term "certificate authority workstation (CAW)".

certification package (C.F.D.)

Product of the certification effort documenting the detailed results of the certification activities.

Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called security assessment report (SAR).

certification practice statement (CPS)

A statement of the practices that a certification authority (CA) employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this Certificate Policy, or requirements specified in a contract for services).

Source: NIST SP 800-32

certification test and evaluation (CT&E)

Software and hardware security tests conducted during development of an information system component.

certified TEMPEST technical authority (CTTA)

An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with CNSS approved criteria and has been appointed by a U.S. Government Department or Agency to fulfill CTTA responsibilities.

Source: CNSSAM TEMPEST/01-13

certifier (C.F.D.)

Individual responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages.

Rationale: Term has been replaced by the term "security control assessor".

chain of custody

A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

Source: NIST SP 800-72

chain of evidence (C.F.D.)

A process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence. The "sequencing" of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner.

Rationale: Sufficiently covered under chain of custody.

chaining

Direct or relayed connections from a higher accredited domain to a series of lower accredited domains without passing through an isolated device that implements the enforcement of all applicable approved policy decisions for each domain transfer.

Source: DoDI 8540.01

challenge and reply authentication

Prearranged procedure in which a subject requests authentication of another and the latter establishes validity with a correct reply.

check word

Cipher text generated by cryptographic logic to detect failures in cryptography.

checksum

A value that (a) is computed by a function that is dependent on the contents of a data object and (b) is stored or transmitted together with the object, for detecting changes in the data.

Source: IETF RFC 4949 Ver 2

chief information officer (CIO)

Agency official responsible for: (1) providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information systems are acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (2) developing, maintaining, and facilitating the implementation of a sound and integrated information system architecture for the agency; and (3) promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

Note: Organizations subordinate to federal agencies may use the term Chief Information Officer to denote individuals filling positions with similar security responsibilities to agency-level Chief Information Officers.

Source: 40 U.S.C. Sec. 1425 (b); NIST SP 800-53 Rev 4

chief information security officer (CISO)

See senior agency information security officer (SAISO).

Source: FIPS PUB 200

cipher

1. Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text, or in which units of plain text are rearranged, or both.

2. Series of transformations that converts plaintext to ciphertext using the Cipher Key.

Source: FIPS PUB 197

cipher text auto-key (CTAK)

Cryptographic logic that uses previous cipher text to generate a key stream.

cipher text/ciphertext

Data in its encrypted form.

See BLACK.

Source: NIST SP 800-57 Part 1 Rev 3

claimant

A party whose identity is to be verified using an authentication protocol.

Source: FIPS PUB 201-1; NIST SP 800-63-2

classified information

See classified national security information.

classified information spillage (C.F.D.)

Security incident that occurs whenever classified data is spilled either onto an unclassified information system or to an information system with a lower level of classification or different security category.

Rationale: Spillage encompasses this term.

classified national security information

Information that has been determined pursuant to Executive Order (E.O.) 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Source: E.O. 13526

clean word list

List of words that have been pre-defined as being acceptable for transmission and may be used in conjunction with a dirty word list to avoid false positives (e.g., secret within secretary). See white list.

clear text

Intelligible data, the semantic content of which is available.

Source: ISO/IEC 7498-2

Note: Clear text data is, by definition, not encrypted.

clearance

A formal security determination by an authorized adjudicative office that an individual is authorized access, on a need to know basis, to a specific level of classified information (TOP SECRET, SECRET, or CONFIDENTIAL).

Source: CNSSI No. 4005 (COMSEC)

clear

A method of sanitization that applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).

Source: NIST SP 800-88 Rev 1

client node

Enables customers to access primary services nodes (PRSNs) to obtain key management infrastructure (KMI) products and services and to generate, produce, and distribute traditional (symmetric) key products. The management client (MGC) configuration of the client node allows customers to operate locally, independent of a PRSN.

Source: CNSSI No. 4005 (COMSEC)

closed security environment

Environment providing sufficient assurance that applications and equipment are protected against the introduction of malicious logic during an information system life cycle. Closed security is based upon a system's developers, operators, and maintenance personnel having sufficient clearances, authorization, and configuration control.

closed storage

The storage of classified information in properly secured General Services Administration-approved security containers.

Source: ICS 700-1

cloud computing

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Source: NIST SP 800-145

coalition partner

A nation in an ad hoc defense arrangement with the U.S.

Source: CNSSI No. 4005 (COMSEC)

code

1. A set of instructions for a computer.

Source: www.merrianwebster.com

2. System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length.

Source: NSTISSI No. 7002

code analysis

The act of reverse-engineering the malicious program to understand the code that implements the software behavior. For example, when looking at compiled programs, the process involves using a disassembler, a debugger, and perhaps a decompiler to examine the program's low-level assembly or byte-code instructions. A disassembler converts the instructions from their binary form into the human-readable assembly form. A decompiler attempts to recreate the original source code of the program. A debugger allows the analyst to step through the code, interacting with it, and observing the effects of its instructions to understand its purpose.

Source: CNSSI No. 1011

codebook

Document containing plain text and code equivalents in a systematic arrangement, or a technique of machine encryption using a word substitution technique.

code group (C.F.D.)

Group of letters, numbers, or both in a code system used to represent a plain text word, phrase, or sentence.

code vocabulary (C.F.D.)

Set of plain text words, numerals, phrases, or sentences for which code equivalents are assigned in a code system.

cognizant security officer/authority

1. An entity charged with responsibility for physical, technical, personnel, and information security affecting that organization.

Source: CNSSI No. 4005 (COMSEC)

2. The single principal designated by a Senior Official of the Intelligence Community (SOIC) to serve as the responsible official for all aspects of security program management concerning the protection of national intelligence, sources and methods, under SOIC responsibility.

Source: ICS 700-1

cold site

A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.

Source: NIST SP 800-34 Rev 1

collateral information

National security information (including intelligence information) classified Top Secret, Secret, or Confidential that is not in the Sensitive Compartmented Information (SCI) or Special Access Program (SAP) category.

Source: ICS 700-1

command authority (CMDAUTH) (COMSEC)

The command authority is responsible for the appointment of user representatives for a department, agency, or organization and their key and granting of modern (electronic) key ordering privileges for those User Representatives.

Source: CNSSI No. 4005 (COMSEC)

commercial COMSEC evaluation program (CCEP)

Relationship between National Security Agency (NSA) and industry, in which NSA provides the COMSEC expertise (i.e., standards, algorithms, evaluations, and guidance) and industry provides design, development, and production capabilities to produce a NSA-approved product. Products developed under the CCEP may include modules, subsystems, equipment, systems, and ancillary devices.

Source: NSA/CSS Manual Number 3-16 (adapted) (COMSEC)

commercial-off-the-shelf (COTS)

A software and/or hardware product that is commercially ready-made and available for sale, lease, or license to the general public.

Source: NSA/CSS Policy 3-14

commercial solutions for classified (CSfC)

A commercial off-the-shelf (COTS) end-to-end strategy and process in which two or more COTS products can be combined into a solution to protect classified information.

Source: NSA/CSS Policy 3-14 (adapted)

commodity service

An information system service (e.g., telecommunications service) provided by a commercial service provider typically to a large and diverse set of consumers. The organization acquiring and/or receiving the commodity service possesses limited visibility into the management structure and operations of the provider, and while the organization may be able to negotiate service-level agreements, the organization is typically not in a position to require that the provider implement specific security controls.

Source: NIST SP 800-53 Rev 4

common access card (CAC)

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

Note: As per DoDI 1000.13, the common access card (CAC), a form of DoD ID card, shall serve as the Federal personal identity verification (PIV) card for DoD implementation of Homeland Security Presidential Directive 12.

Source: DoDI 1000.13 (adapted)

common carrier

In a telecommunications context, a telecommunications company that holds itself out to the public for hire to provide communications transmission services.

Note: In the United States, such companies are usually subject to regulation by federal and state regulatory commissions.

Source: NIST SP 800-53 Rev 4

common configuration enumeration (CCE)

A nomenclature and dictionary of software security configurations.

Source: NIST SP 800-126 Rev 2

common control

A security control that is inherited by one or more organizational information systems.

See security control inheritance.

Source: NIST SP 800-37 Rev 1

common control provider

An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems).

Source: NIST SP 800-37 Rev 1; NIST SP 800-53 Rev 4

common criteria

Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems.

common fill device (CFD)

Any one of a family of devices developed to read-in, transfer, or store key.

Source: NSA/CSS Manual Number 3-16 (adapted) (COMSEC)

common platform enumeration (CPE)

A nomenclature and dictionary of hardware, operating systems, and applications.

Source: NIST SP 800-126 Rev 2

common services provider (CSP)

A federal organization that provides National Security System-Public Key Infrastructure (NSS-PKI) support to other federal organizations, academia and industrial partners requiring classified NSS-PKI support but without their own self-managed infrastructures.

Source: CNSSD No. 507

common user application software (CUAS)

User application software developed to run on top of the local COMSEC management software (LCMS) on the local management device/key processor (LMD/KP).

Source: CNSSI No. 4005 (COMSEC)

common vulnerabilities and exposures (CVE)

A nomenclature and dictionary of security-related software flaws.

Source: NIST SP 800-126 Rev 2

common vulnerability scoring system (CVSS)

A system for measuring the relative severity of software flaw vulnerabilities.

Source: NIST SP 800-126 Rev 2

common weakness enumeration (CWE)

A taxonomy for identifying the common sources of software flaws (e.g., buffer overflows, failure to check input data).

Source: NIST ITL Bulletin, Dec. 2013

communications cover

See cover (TRANSEC).

communications deception (C.F.D.)

Deliberate transmission, retransmission, or alteration of communications to mislead an adversary's interpretation of the communications.

Rationale: Partner terms (imitative communications deception and manipulative communications deception) were listed for deletion in 2010 version of CNSS 4009.

communications profile

Analytic model of communications associated with an organization or activity. The model is prepared from a systematic examination of communications content and patterns, the functions they reflect, and the communications security measures applied.

communications security (COMSEC)

A component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emissions security, and physical security of COMSEC material.

Source: CNSSI No. 4005 (COMSEC)

community of interest (COI)

A collaborative group of users who exchange information in pursuit of their shared goals, interests, missions, or business processes, and who therefore must have a shared vocabulary for the information they exchange. The group exchanges information within and between systems to include security domains.

community risk

Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population.

compartmentalization

A nonhierarchical grouping of information used to control access to data more finely than with hierarchical security classification alone.

competent security official

Any cognizant security authority or person designated by the cognizant security authority.

Source: CNSSI No. 4005 (COMSEC)

compensating security control

The security controls employed in lieu of the recommended controls in the security control baselines described in NIST Special Publication 800-53 and CNSS Instruction 1253 that provide equivalent or comparable protection for an information system or organization.

Source: NIST SP 800-53 Rev 4 (adapted)

composed commercial solution

Two or more commercial Information Assurance (IA) products layered together to address the security requirements of an operational use case according to National Security Agency (NSA) guidance. A composed solution, once approved by NSA, may take the place of a single certified Government-off-the-Shelf (GOTS) IA product to provide the confidentiality and/or other security services necessary to protect National Security Systems.

Source: CNSSI No. 4031

comprehensive testing

A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as white box testing.

Source: NIST SP 800-53A Rev 1

compromise

1. Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Source: NIST SP 800-32

2.
a. (General) the disclosure of classified data to persons not authorized to receive that data.
b. (Automated Information Systems) A violation of the security policy of a system such that an unauthorized disclosure, modification, or destruction of sensitive information has occurred.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

compromised key list (CKL)

The set of Key Material Identification Numbers (KMIDs) of all keys in a universal that have been reported compromised. Cryptographic devices will not establish a secure connection with equipment whose KMID is on the CKL.

Source: CNSSI No. 4032

compromising emanations

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

Source: CNSSAM TEMPEST/01-13

computer abuse

Intentional or reckless misuse, alteration, disruption, or destruction of information processing resources.

computer cryptography

Use of a crypto-algorithm program by a computer to authenticate or encrypt/decrypt information.

computer forensics

See digital forensics.

computer incident response team (CIRT)

Group of individuals usually consisting of security analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Cyber Incident Response Team, Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center or Computer Incident Response Capability).

computer network attack (CNA)

Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Note: Within DoD, Joint Publication 3-13, "Information Operations, " 27 November 2012 approved the removal the terms and definitions of computer network attack (CNA), computer network defense (CND), computer network exploitation, and computer network operations (CNO) from JP -1-02, "Department of Defense Dictionary of Military Terms and Associated Terms." This term and definition is no longer published in JP 1-02. This publication is the primary terminology source when preparing correspondence, to include policy, strategy, doctrine, and planning documents. The terms are no longer used in issuances being updated within DoD. JP 1-02, following publication of JP 3-12, "Cyberspace Operations" provides new terms and definitions such as cyberspace, cyberspace operations, cyberspace superiority, defensive cyberspace operation response action, defensive cyberspace operations, Department of Defense information network operations, and offensive cyberspace operations.

computer network defense (CND)

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

Note: Within DoD, term was approved for deletion from JP 1-02 (DoD Dictionary) by issuance of JP 3-13, "Information Operations". This term has been replaced by the use of “cyberspace defense" used in JP 3-12, "Cyberspace Operations." Original source of term was JP 1-02 (DoD Dictionary).

computer network exploitation (CNE)

Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks.

Note: Within the Department of Defense (DoD), term was approved for deletion from JP 1-02 (DoD Dictionary). Original source of term was JP 1-02 (DoD Dictionary). The military no longer uses this term to describe these operations, but it is still used outside of military operations.

computer network operations (CNO)

Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.

Note: Within the Department of Defense (DoD), term was approved for deletion from JP 1-02 (DoD Dictionary). This term has been replaced by the use of " cyberspace operations" used in JP 3-12, "Cyberspace Operations." Original source of term was JP 1-02 (DoD Dictionary).

computer security (COMPUSEC) (C.F.D.)

Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

Rationale: Term has been replaced by the term “cybersecurity”.

computer security incident (C.F.D.)

See incident.

Source: NIST IR 7298 Rev 2

computer security object (C.F.D.)

A resource, tool, or mechanism used to maintain a condition of security in a computerized environment. These objects are defined in terms of attributes they possess, operations they perform or are performed on them, and their relationship with other objects.

Source: FIPS PUB 188

computer security objects register (C.F.D.)

A collection of computer security object (CSO) names and definitions kept by a registration authority.

Source: FIPS PUB 188

computer security subsystem (C.F.D.)

Hardware/software designed to provide computer security features in a larger system environment.

computerized telephone system (CTS)

A generic term used to describe any telephone system that uses centralized stored program computer technology to provide switched telephone networking features and services. CTSs are referred to commercially, by such terms, as: computerized private branch exchange (CPBX); private branch exchange (PBX); private automatic branch exchange (PABX); electronic private automatic branch exchange (EABX); computerized branch exchange (CBX); computerized key telephone systems (CKTS); hybrid key systems; business communications systems; and office communications systems.

Source: CNSSI No. 5002

computing environment

Workstation or server (host) and its operating system, peripherals, and applications.

COMSEC account

An administrative entity identified by an account number, used to maintain accountability, custody and control of COMSEC material.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

COMSEC account audit

Inventory and reconciliation of the holdings, records, and procedures of a COMSEC account ensuring all accountable COMSEC material is properly handled and safeguarded.

Source: NSA/CSS Manual Number 3-16 (adapted) (COMSEC)

COMSEC account manager

An individual designated by proper authority to be responsible for the receipt, transfer, accountability, safeguarding, and destruction of COMSEC material assigned to a COMSEC account. This applies to both primary accounts and subaccounts. The equivalent key management infrastructure (KMI) position is the KMI operating account (KOA) manager.

Source: CNSSI No. 4005 (COMSEC)

COMSEC aids

All COMSEC material other than equipment or devices, which assist in securing telecommunications and is required in the production, operation, and maintenance of COMSEC systems and their components. Some examples are: COMSEC keying material, and supporting documentation, such as operating and maintenance manuals.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

COMSEC assembly (C.F.D.)

Group of parts, elements, subassemblies, or circuits that are removable items of COMSEC equipment.

Rationale: The term falls under the broader term “COMSEC material”.

COMSEC boundary (C.F.D.)

Definable perimeter encompassing all hardware, firmware, and software components performing critical COMSEC functions, such as key generation, handling, and storage.

Rationale: The term falls under the broader term “COMSEC material”.

COMSEC chip set (C.F.D.)

Collection of NSA approved microchips.

Rationale: The term falls under the broader term “COMSEC material”.

COMSEC control program (C.F.D.)

Computer instructions or routines controlling or affecting the externally performed functions of key generation, key distribution, message encryption/decryption, or authentication.

Rationale: The term falls under the broader term “COMSEC material”.

COMSEC custodian (C.F.D.)

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

Source: NSA/CSS Manual Number 3-16 (COMSEC)

Rationale: Term has been replaced by the term “COMSEC account manager”.

COMSEC demilitarization (C.F.D.)

Process of preparing COMSEC equipment for disposal by extracting all controlled cryptographic item (CCI), classified, or CRYPTO marked components for their secure destruction, as well as defacing and disposing of the remaining equipment hulk.

Rationale: Demilitarize is the proper term and does not apply solely to COMSEC.

COMSEC element (C.F.D.)

Removable item of COMSEC equipment, assembly, or subassembly; normally consisting of a single piece or group of replaceable parts.

Rationale: The term falls under the broader term “COMSEC material”.

COMSEC emergency

A tactical operational situation, as perceived by the responsible person/officer in charge, in which the alternative to strict compliance with procedural restrictions affecting use of a COMSEC equipment would be plain text communication.

Source: NSA NAG 16F

COMSEC end-item

Equipment or combination of components ready for use in a COMSEC application.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

COMSEC equipment

Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and, subsequently, by reconverting such information to its original form for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the conversion process. COMSEC equipment includes cryptographic-equipment, crypto-ancillary equipment, cryptographic production equipment, and authentication equipment.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

COMSEC facility

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

Source: CNSSI No. 4005 (COMSEC)

COMSEC incident

Any occurrence that potentially jeopardizes the security of COMSEC material or the secure transmission of national security information. COMSEC Incident includes Cryptographic Incident, Personnel Incident, Physical Incident, and Protective Technology/Package Incident.

Source: CNSSI No. 4005 (COMSEC); NSA/CSS Manual Number 3-16 (COMSEC)

COMSEC Incident Monitoring Activity (CIMA)

The office within a department or agency maintaining a record of COMSEC incidents caused by elements of that department or agency, and ensuring all actions required of those elements are completed.

Source: CNSSI No. 4006; CNSSI No. 4032

COMSEC insecurity

A COMSEC incident that has been investigated, evaluated, and determined to jeopardize the security of COMSEC material or the secure transmission of information.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

COMSEC manager (C.F.D.)

Individual who manages the COMSEC resources of an organization.

Rationale: The more accurate and used term is “COMSEC account manager”.

COMSEC material

Item(s) designed to secure or authenticate telecommunications. COMSEC material includes, but is not limited to key, equipment, modules, devices, documents, hardware, firmware, or software that embodies or describes cryptographic logic and other items that perform COMSEC functions. This includes Controlled Cryptographic Item (CCI) equipment, Cryptographic High Value Products (CHVP) and other Suite B equipment, etc.

Source: CNSSI No. 4005 (COMSEC)

COMSEC material control system (CMCS)

The logistics and accounting system through which COMSEC material marked CRYPTO is distributed, controlled, and safeguarded. Included are the COMSEC central offices of record (COR), cryptologistic depots, and COMSEC accounts. COMSEC material other than key may be handled through the CMCS. Electronic Key Management System (EKMS) and Key Management Infrastructure (KMI) are examples of tools used by the CMCS to accomplish its functions.

Source: CNSSI No. 4005 (COMSEC)

COMSEC module (C.F.D.)

Removable component that performs COMSEC functions in a telecommunications equipment or system.

Rationale: The term falls under the broader term “COMSEC material”.

COMSEC monitoring

The act of listening to, copying, or recording transmissions of one's own official telecommunications to provide material for analysis in order to determine the degree of security being provided to those transmissions.

Source: NTISSD 600

COMSEC profile (C.F.D.)

Statement of COMSEC measures and materials used to protect a given operation, system, or organization.

Rationale: No known reference for this term.

COMSEC service authority

See service authority.

Source: CNSSI No. 4005 (COMSEC)

COMSEC software

Includes all types of COMSEC material, except key, in electronic or physical form. This includes all classifications of unencrypted software, and all associated data used to design, create, program, or run that software. It also, includes all types of source/executable/object code and associated files that implement, execute, embody, contain, or describe cryptographic mechanisms, functions, capabilities, or requirements. COMSEC software also includes transmission security (TRANSEC) software and may include any software used for purposes of providing confidentiality, integrity, authentication, authorization, or availability services to information in electronic form.

Source: CNSSI No. 4005 (COMSEC)

COMSEC survey (C.F.D.)

Organized collection of COMSEC and communications information relative to a given operation, system, or organization.

Rationale: No known reference for this term.

COMSEC system data (C.F.D.)

Information required by a COMSEC equipment or system to enable it to properly handle and control key.

Rationale: No known reference for this term.

COMSEC training

Teaching of skills relating to COMSEC accounting and the use of COMSEC aids.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

concept of operations (CONOP)

See security concept of operations.

confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Source: 44 U. S. Code Sec 3542

configuration control

Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications prior to, during, and after system implementation.

Source: NIST SP 800-37 Rev 1

configuration control board (CCB)

Establishment of and charter for a group of qualified people with responsibility for the process of controlling and approving changes throughout the development and operational lifecycle of products and systems; may also be referred to as a change control board.

configuration item

An aggregation of information system components that is designated for configuration management and treated as a single entity in the configuration management process.

Source: NIST SP 800-53 Rev 4

configuration management

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

Source: NIST SP 800-53 Rev 4

configuration settings

The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the information system.

Source: NIST SP 800-53 Rev 4

consent banner

See security banner (also known as notice and consent banners)

contamination

See spillage.

content signing certificate

A certificate issued for the purpose of digitally signing information (content) to confirm the author and guarantee that the content has not been altered or corrupted since it was signed by use of a cryptographic hash.

Source: CNSSI No. 1300

contingency key

Key held for use under specific operational conditions or in support of specific contingency plans.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

contingency plan

Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the continuity of operations plan (COOP) or disaster recovery plan (DRP) for major disruptions.

continuity of government (COG)

A coordinated effort within the Federal Government's executive branch to ensure that national essential functions continue to be performed during a catastrophic emergency.

continuity of operations plan (COOP)

A predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.

Source: NIST SP 800-34 Rev 1

continuous monitoring

Maintaining ongoing awareness to support organizational risk decisions.
See information security continuous monitoring, risk monitoring, and status monitoring

Source: NIST SP 800-137

control correlation identifier (CCI)

Decomposition of a National Institute of Standards and Technology (NIST) control into a single, actionable, measurable statement.

Source: DoDI 8500.01

controlled access area

The complete building or facility area under direct physical control within which unauthorized persons are denied unrestricted access and are either escorted by authorized personnel or are under continuous physical or electronic surveillance.

Source: NSTISSI No. 7003

controlled access protection (C.F.D.)

Minimum set of security functionality that enforces access control on individual users and makes them accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation.

Rationale: Controlled access protection was described in the Controlled Access Protection Profile (CAPP) of October 1999 implementing C2. As the CAPP was superseded by the General Purpose Operating System Profile, the CAPP definition should be deleted.

controlled area

Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

Source: NIST SP 800-53 Rev 4

controlled cryptographic item (CCI)

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

Source: NSA/CSS Manual Number 3-16 (COMSEC)

controlled cryptographic item (CCI) assembly

A device approved by the National Security Agency (NSA) as a controlled cryptographic item, that embodies a cryptographic logic or other cryptographic design, and performs the entire COMSEC function, but is dependent upon the host equipment to operate.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

controlled cryptographic item (CCI) component

A device approved by the National Security Agency as a controlled cryptographic item that embodies a cryptographic logic or other cryptographic design, and does not perform the entire the COMSEC function but is dependent upon a host equipment or assembly, to complete and operate the COMSEC function.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

controlled cryptographic item (CCI) equipment

A telecommunications or information handling equipment that embodies a CCI component or CCI assembly and performs the entire COMSEC function without dependence on host equipment to operate.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

controlled interface

A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems.

Source: NIST SP 800-37 Rev 1; NIST SP 800-53 Rev 4

controlled space

Three-dimensional space surrounding information system equipment, within which unauthorized individuals are denied unrestricted access and are either escorted by authorized individuals or are under continuous physical or electronic surveillance.

controlled unclassified information (CUI)

Information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, *Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

Source: E.O. 13556 (adapted)

Note: The CUI categories and subcategories are listed in the CUI Registry, available at www.archives.gov/cui.

controlled unclassified information (CUI) registry

The online repository of information and policy regarding how authorized holders of CUI should handle such information.

Note: The Controlled Unclassified Information (CUI) Registry: (i) identifies all categories and subcategories of information that require safeguarding or dissemination controls consistent with law, regulation and Government-wide policies; (ii) provides descriptions for each category and subcategory; (iii) identifies the basis for safeguarding and dissemination controls;(iv) contains associated markings and applicable safeguarding, disseminating, and (v) specifies CUI that may be originated only by certain executive branch agencies and organizations. The CUI Executive Agent is the approval authority for all categories/subcategories of information identified as CUI in the CUI Registry and only those categories/subcategories listed are considered CUI.

Source: E.O. 13556 (adapted)

controlling authority (CONAUTH)

The official responsible for directing the operation of a cryptonet using traditional key and for managing the operational use and control of keying material assigned to the cryptonet.

Source: NSA/CSS Manual Number 3-16 (COMSEC) (adapted)

controlling domain

The domain that assumes the greater risk and thus enforces the most restrictive policy.

cookie
A piece of state information supplied by a Web server to a browser, in a response for a requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests.

Source: NIST SP 800-28

cooperative key generation (CKG)
Electronically exchanging functions of locally generated, random components, from which both terminals of a secure circuit construct traffic encryption key or key encryption key for use on that circuit. See per-call key.

cooperative remote rekeying
Synonymous with manual remote rekeying.

correctness proof
A mathematical proof of consistency between a specification and its implementation.

counterintelligence
Counterintelligence means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.
Source: E.O. 12333 (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008))

countermeasures
Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.

Source: NIST 800 SP 800-37 Rev 1; FIPS PUB 200

courier
A duly authorized and trustworthy individual who has been officially designated to transport/carry material, and if the material is classified, is cleared to the level of material being transported.

Source: CNSSI No. 4005 (COMSEC) (adapted)

course of action (risk response)
A time-phased or situation-dependent combination of risk response measures. See risk response.

Source: NIST SP 800-39

cover (TRANSEC)
Result of measures used to obfuscate message externals to resist traffic analysis.

Source: CNSSI No. 1200

coverage
An attribute associated with an assessment method that addresses the scope or breadth of the assessment objects included in the assessment (e.g., types of objects to be assessed and the number of objects to be assessed by type). The values for the coverage attribute, hierarchically from less coverage to more coverage, are basic, focused, and comprehensive.

Source: NIST SP 800-53A Rev 1; NIST SP 800-137

covert channel
An unintended or unauthorized intra-system channel that enables two cooperating entities to transfer information in a way that violates the system's security policy but does not exceed the entities' access authorizations.

Source: IETF RFC 4949 Ver 2

covert channel analysis

Determination of the extent to which the security policy model and subsequent lower-level program descriptions may allow unauthorized access to information.

covert storage channel

A system feature that enables one system entity to signal information to another entity by directly or indirectly writing a storage location that is later directly or indirectly read by the second entity. See: covert channel.

Source: IETF RFC 4949 Ver 2

covert timing channel

A system feature that enables one system entity to signal information to another by modulating its own use of a system resource in such a way as to affect system response time observed by the second entity. See: covert channel.

Source: IETF RFC 4949 Ver 2

credential

1. Evidence or testimonials that support a claim of identity or assertion of an attribute and usually are intended to be used more than once.

2. Evidence attesting to one's right to credit or authority.

Source: FIPS PUB 201-1

3. An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token processed and controlled by a Subscriber.

Source: NIST SP 800-63-2

credential service provider (CSP)

A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass registration authorities (RAs) and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.

Source: NIST SP 800-63-2

critical component

A component which is or contains information and communications technology (ICT), including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system.

Source: DoDI 5200.44

critical infrastructure

System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

critical infrastructure sectors

Information technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping.

Source: NIST SP 800-30 Rev 1

critical security parameter

Security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and personal identification numbers (PINs)) whose disclosure or modification can compromise the security of a cryptographic module.

Source: FIPS PUB 140-2

criticality

A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.

Source: NIST SP 800-60 Vol 1 Rev 1

criticality analysis

An end-to-end functional decomposition performed by systems engineers to identify mission critical functions and components. Includes identification of system missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system missions(s).

Source: DoDI 5200.44

criticality level

Refers to the (consequences of) incorrect behavior of a system. The more serious the expected direct and indirect effects of incorrect behavior, the higher the criticality level.

cross certificate

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

Note: This is a more narrow definition than described in X.509.

Source: CNSSI No. 1300

cross domain

The act of manually and/or automatically accessing and/or transferring information between different security domains.

Source: DoDI 8540.01

cross domain baseline list

A list managed by the unified cross domain services management office (UCDSMO) that identifies CDSs that are available for deployment within the Department of Defense (DoD) and intelligence community (IC).

Source: DoDI 8540.01

cross domain capabilities

The set of functions that enable the transfer of information between security domains in accordance with the policies of the security domains involved.

cross domain enabled

Applications/services that exist on and are capable of interacting across two or more different security domains.

cross domain portal

A single web-site providing access to cross domain services.

cross domain service

Services that provide access and/or transfer of information between different security domains.

cross domain solution (CDS)

A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains.

Source: NIST SP 800-37 Rev 1; NIST SP 800-53 Rev 4; CNSSI No. 1253F Attachment 3

cross domain solution (CDS) filtering

The process of inspecting data as it traverses a cross domain solution and determines if the data meets pre-defined policy.

cross domain sunset list

A list managed by the unified cross domain services management office (UCDSMO) that identifies cross domain solutions (CDSs) that are or have been in operation, but are no longer available for additional deployment and need to be replaced within a specified period of time.

Source: DoDI 8540.01

cross-certificate

1. A certificate used to establish a trust relationship between two certification authorities.

Source: NIST SP 800-32

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

Source: CNSSI No. 1300

cryptanalysis

1. Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection.
2. The study of mathematical techniques for attempting to defeat cryptographic techniques and/or information systems security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself.

Source: NIST SP 800-57 Part 1 Rev 3

CRYPTO

The marking or designator identifying unencrypted COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. Government or U.S. Government-derived information. This includes non-split keying material used to encrypt/decrypt COMSEC critical software and software based algorithms.

Source: CNSSI No. 4005 (COMSEC)

cryptographic

Pertaining to, or concerned with, cryptography.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

cryptographic alarm

Circuit or device that detects failures or aberrations in the logic or operation of cryptographic equipment. Crypto-alarm may inhibit transmission or may provide a visible and/or audible alarm.

cryptographic algorithm (crypto-algorithm)

1. A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output.

Source: NIST SP 800-57 Part 1 Rev 3

2. Well-defined procedure or sequence of rules or steps, or a series of mathematical equations used to describe cryptographic processes such as encryption/decryption, key generation, authentication, signatures, etc.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

cryptographic ancillary equipment (crypto-ancillary equipment)

Equipment designed specifically to facilitate efficient or reliable operation of cryptographic equipment, but which does not itself perform cryptographic functions.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

cryptographic binding

Associating two or more related elements of information using cryptographic techniques.

cryptographic boundary

Explicitly defined continuous perimeter that establishes the physical and/or logical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.

Source: ISO/IEC 19790

cryptographic component

The hardware or firmware embodiment of the cryptographic logic in a secure telecommunications or automated information processing system. A cryptographic component may be a modular assembly, a printed wiring assembly (PWA), a microcircuit, or a combination of these items.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

cryptographic equipment (cryptoequipment)

Equipment that embodies a cryptographic logic.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

cryptographic erase

A method of sanitization in which the media encryption key (MEK) for the encrypted Target Data is sanitized, making recovery of the decrypted Target Data infeasible.

Source: NIST SP 800-88 Rev 1

cryptographic high value product (CHVP)

NSA-approved products incorporating only UNCLASSIFIED components and UNCLASSIFIED cryptographic algorithms. This does include COTS, products approved by NSA, but does not include composed commercial solutions or their components, unless an individual component has been approved as a CHVP. Unkeyed CHVPs are not classified or designated as controlled cryptographic item (CCI).

Source: CNSSI No. 4031

cryptographic ignition key (CIK)

Device or electronic key used to unlock the secure mode of cryptographic equipment.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

cryptographic incident

Any uninvestigated or unevaluated equipment malfunction or operator or COMSEC Account Manager error that has the potential to jeopardize the cryptographic security of a machine, off-line manual cryptosystem OR any investigated or evaluated occurrence that has been determined as not jeopardizing the cryptographic security of a cryptosystem.

Source: CNSSI No. 4006

cryptographic initialization

Function used to set the state of a cryptographic logic prior to key generation, encryption, or other operating mode.

cryptographic logic

The embodiment of one (or more) cryptographic algorithm(s) along with alarms, checks, and other processes essential to effective and secure performance of the cryptgraphic process(es).

Note: In non-technical terms, a comprehensive and precisely defined sequence of steps or procedural rules used to produce cipher text from plain text and vice versa.

Source: CNSSI No. 4005 (COMSEC); NSA/CSS Manual Number 3-16 (COMSEC)

cryptographic material (cryptomaterial) (slang CRYPTO)

All material, including documents, devices, or equipment that contains cryptographic information and is essential to the encryption, decryption, or authentication of telecommunications.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

cryptographic net (cryptonet)

Stations that hold a common key.

Source: CNSSI No. 4005 (COMSEC); NSA/CSS Manual Number 3-16 (COMSEC)

cryptographic period (cryptoperiod)

The time span during which each key setting remains in effect.

Source: CNSSI No. 4005 (COMSEC); NSA/CSS Manual Number 3-16 (COMSEC)

cryptographic product

A cryptographic key (public, private, or shared) or public key certificate, used for encryption, decryption, digital signature, or signature verification; and other items, such as compromised key lists (CKL) and certificate revocation lists (CRL), obtained by trusted means from the same source which validate the authenticity of keys or certificates. Protected software which generates or regenerates keys or certificates may also be considered a cryptographic product.

cryptographic randomization

Function that randomly determines the transmit state of a cryptographic logic.

cryptographic security (cryptosecurity)

Component of COMSEC that results from the provision of technically sound cryptographic systems and their proper use.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

cryptographic solution

The generic term for a cryptographic device, COMSEC equipment, or combination of such devices/equipment containing either a classified algorithm or an unclassified algorithm.

Source: CNSSI No. 4005 (COMSEC)

cryptographic synchronization

Process by which a receiving decrypting cryptographic logic attains the same internal state as the transmitting encrypting logic.

cryptographic system (cryptosystem)

Associated information security (INFOSEC) items interacting to provide a single means of encryption or decryption.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

cryptographic system analysis

Process of establishing the exploitability of a cryptographic system, normally by reviewing transmitted traffic protected or secured by the system under study.

cryptographic system evaluation

Process of determining vulnerabilities of a cryptographic system and recommending countermeasures.

cryptographic system review

Examination of a cryptographic system by the controlling authority ensuring its adequacy of design and content, continued need, and proper distribution.

cryptographic system survey

Management technique in which actual holders of a cryptographic system express opinions on the system's suitability and provide usage information for technical evaluations.

cryptographic token

1. A portable, user-controlled, physical device (e.g., smart card or PC card) used to store cryptographic information and possibly also perform cryptographic functions.

2. A token where the secret is a cryptographic key.

Source: NIST SP 800-63-2

cryptography

1. Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

2. The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.

Source: NIST SP 800-59

3. The discipline that embodies the principles, means, and methods for the providing information security, including confidentiality, data integrity, non-repudiation, and authenticity.

Source: NIST SP 800-21 2nd edition

cryptologic

Of or pertaining to cryptology.

Source: NIST SP 800-59

cryptology

The mathematical science that deals with cryptanalysis and cryptography.

cryptonet evaluation report

A free form message from the electronic key management system (EKMS) Tier 1 that includes the Controlling Authority’s ID and Name, Keying Material Information, Description/Cryptonet Name, Remarks, and Authorized User Information.

Source: CNSSI No. 4006

cyber incident

Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein. See incident. See also event, security-relevant event, and intrusion.

cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Source: NSPD-54/HSPD-23

cyberspace

The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

Source: NSPD-54/HSPD-23

cyberspace attack

Cyberspace actions that create various direct denial effects (i.e. degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains.

Source: DoD JP 3-12

cyberspace capability

A device, computer program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace.

Source: DoD JP 3-12

cyberspace defense

Actions normally created within DoD cyberspace for securing, operating, and defending the DoD information networks. Specific actions include protect, detect, characterize, counter, and mitigate.

Source: DoDI 8500.01

cyberspace operations (CO)

The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

Source: DoD JP 3-0

cyberspace superiority

The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary.

Source: DoD JP 3-12

cyclic redundancy check (CRC)

A type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service where accidental changes to data are expected.

Source: IETF RFC 4949 Ver 2

data

Information in a specific representation, usually as a sequence of symbols that have meaning.

Source: IETF RFC 4949 Ver 2

data aggregation

Compilation of individual data systems and data that could result in the totality of the information being classified, or classified at a higher level, or of beneficial use to an adversary.

data asset

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

2. An information-based resource.

data element

A basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location.

Source: NIST SP 800-47

data flow control

See with information flow control.

data governance

A set of processes that ensures that data assets are formally managed throughout the enterprise. A data governance model establishes authority and management and decision making parameters related to the data produced or managed by the enterprise.

Source: NSA/CSS Policy 11-1

data integrity

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

Source: NIST SP 800-27 Rev A

data loss

The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.

Source: NIST SP 800-137

data loss prevention

A systems ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of NSS information.

Source: CNSSI No. 1011

data mining

An analytical process that attempts to find correlations or patterns in large data sets for the purpose of data or knowledge discovery.

Source: NIST SP 800-53 Rev 4

data origin authentication

The corroboration that the source of data received is as claimed~~.~~

See also non-repudiation and peer entity authentication service

Source: IETF RFC 4949 Ver 2

data provenance

In the context of computers and law enforcement use, it is an equivalent term to chain of custody. It involves the method of generation, transmission and storage of information that may be used to trace the origin of a piece of information processed by community resources.

Source: ISA SSA (adapted)

data spillage

See spillage.

data tag

A non-hierarchical keyword or term assigned to a piece of information which helps describe an item and allows it to be found or processed automatically.

Source: ISA SSA

data transfer device (DTD) (COMSEC)

Fill device designed to securely store, transport, and transfer electronically both COMSEC and TRANSEC key, designed to be backward compatible with the previous generation of COMSEC common fill devices, and programmable to support modern mission systems.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

data transfer solution

Interconnect networks or information systems that operate in different security domains and transfer data between them.

Source: DoDI 8540.01

decertification

Revocation of the certification of an information system item or equipment for cause.

decipher

Convert enciphered text to plain text by means of a cryptographic system.

decode

Convert encoded data back to its original form of representation.

Source: IETF RFC 4949 Ver 2

decrypt

A generic term encompassing decoding and deciphering.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

default classification

Classification reflecting the highest classification being processed in an information system. Default classification is included in the caution statement affixed to an object.

defense-in-breadth

A planned, systematic set of multi-disciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component lifecycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).

defense-in-depth

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

Source: NIST SP 800-53 Rev 4

defensive cyberspace operations (DCO)

Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.

Source: DoD JP 3-12

defensive cyberspace operation response action (DCO-RA)

Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense (DoD) cyberspace capabilities or other designated systems.

Source: DoD JP 3-12

degauss

To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing.

Source: NIST SP 800-88 Rev 1

deleted file

A file that has been logically, but not necessarily physically, erased from the operating system, perhaps to eliminate potentially incriminating evidence. Deleting files does not always necessarily eliminate the possibility of recovering all or part of the original data.

Source: NIST SP 800-72

delivery-only client (DOC) (C.F.D.)

A configuration of a client node that enables a DOA agent to access a primary services node (PRSN) to retrieve KMI products and access KMI services. A DOC consists of a client platform but does not include an AKP.

Rationale: Term is of limited use to information assurance community.

demilitarize

The process of preparing National Security System equipment for disposal by extracting all CCI, classified, or CRYPTO-marked components for their secure destruction, as well as defacing and disposing of the remaining equipment hulk.

Source: CNSSI No. 4004.1 (adapted)

demilitarized zone (DMZ)

1. Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance (IA) policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

2. A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet.

Source: NIST SP 800-45 Ver 2

3. An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied.

Source: NIST SP 800-41 Rev 1

denial of service (DoS)

The prevention of authorized access to resources or the delaying of time- critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Source: NIST SP 800-27 Rev A

Department of Defense information network operations

Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks.

Source: JP 3-12

Department of Defense information networks (DODIN)

The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.

Source: JP 1-02, JP 3-12

depth

An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method. The values for the depth attribute, hierarchically from less depth to more depth, are basic, focused, and comprehensive.

Source: NIST SP 800-137

derived credential

A credential issued based on proof of possession and control of a token associated with a previously issued credential, so as not to duplicate the identity proofing process.

Source: NIST SP 800-63-2

designated approval authority (DAA) (C.F.D.)

Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with authorizing official, designated accrediting authority, and delegated accrediting authority.

Rationale: Term has been replaced by the term “authorizing official”.

destroy

A method of sanitization that renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

Source: NIST SP 800-88 Rev 1

developer

A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; (iv) and product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities.

Source: NIST SP 800-53 Rev 4

device distribution profile

An approval-based access control list (ACL) for a specific product that 1) names the user devices in a specific KMI operating account (KOA) to which primary services nodes (PRSNs) distribute the product and 2) states conditions of distribution for each device.

device registration manager

The management role that is responsible for performing activities related to registering users that are devices.

digital forensics

In its strictest connotation, the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony.

Source: DoDD 5505.13E

digital media

A form of electronic media where data are stored in digital (as opposed to analog) form.

Source: NIST SP 800-53 Rev 4

digital signature

The result of a cryptographic transformation of data that, when properly implemented, provides the services of: 1. origin authentication, 2. data integrity, and 3. signer non-repudiation.

Source: FIPS PUB 140-2; NIST SP 800-57 Part 1 Rev 3

direct BLACK wireline

A BLACK metallic wireline that directly leaves the inspectable space in a continuous electrical path with no signal interruption or isolation. Continuous wirelines may be patched or spliced. Examples of wirelines that directly leave the inspectable space are analog telephone lines, commercial television cables, and alarm lines. Wirelines that do not leave the inspectable space are wirelines that pass through a digital switch or converter that reestablishes the signal level or reformats the signaling. Examples of BLACK wirelines that do not directly leave the inspectable space are telephone lines that connect to digital telephone switches, Ethernet lines that connect to digital network routers and alarm lines that connect to an alarm panel.

Source: CNSSAM TEMPEST/01-13

directory service (D/S)

Repository of account registration.

Source: CNSSI No. 4005 (COMSEC)

dirty word list

List of words that have been pre-defined as being unacceptable for transmission and may be used in conjunction with a clean word list to avoid false negatives (e.g., secret within secretary).

disaster recovery plan (DRP)

1. Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by the enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days. See continuity of operations plan (COOP) and contingency plan.

2. A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

Source: NIST SP 800-34 Rev 1

discretionary access control (DAC)

An access control policy that is enforced over all subjects and objects in an information system where the policy specifies that a subject that has been granted access to information can do one or more of the following: (i) pass the information to other subjects or objects; (ii) grant its privileges to other subjects; (iii) change security attributes on subjects, objects, information systems, or system components; (iv) choose the security attributes to be associated with newly-created or revised objects; or (v) change the rules governing access control. Mandatory access controls restrict this capability.

Source: NIST SP 800-53 Rev 4

disruption

An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

Source: NIST SP 800-34 Rev 1 (adapted)

distinguished name (DN)

An identifier that uniquely represents an object in the X.500 directory information tree.

Source: IETF RFC 4949 Ver 2

distinguishing identifier

Information which unambiguously distinguishes an entity in the authentication process.

Source: FIPS PUB 196

distributed denial of service (DDoS)

A denial of service technique that uses numerous hosts to perform the attack.

DoD information

Any information that has not been cleared for public release in accordance with Department of Defense (DoD) Directive 5230.09, “Clearance of DoD Information for Public Release”, and that has been collected, developed, received, transmitted, used, or stored by DoD, or by a non-DoD entity in support of an official DoD activity.

Source: DoDI 8500.01

domain

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

Source: NIST SP 800-53 Rev 4

dynamic subsystem

A subsystem that is not continually present during the execution phase of an information system. Service-oriented architectures and cloud computing architectures are examples of architectures that employ dynamic subsystems.

Source: NIST SP 800-37 Rev 1; NIST SP 800-53 Rev 4

e-government (e-gov) (C.F.D.)

The use by the U.S. Government of web-based Internet applications and other information technology.

Rationale: General definition of a commonly understood term

effective period

Time span during which each COMSEC key edition (i.e., multiple key segments) remains in effect.

Source: CNSSI No. 4006 (adapted)

electronic authentication (e-authentication)

The process of establishing confidence in user identities electronically presented to an information system.

Source: NIST SP 800-63-2

electronic business (e-business) (C.F.D.)

Doing business online.

Rationale: Term is general and not specific to IA.

electronic credentials

Digital documents used in authentication that bind an identity or an attribute to a subscriber's authenticator.

electronic fill device (EFD)

A COMSEC item used to transfer or store key in electronic form or to insert key into cryptographic equipment.

Source: CNSSI No. 4006

electronic key management system (EKMS)

An interoperable collection of systems that automate the planning, ordering, generating, distributing, storing, filling, using, and destroying of electronic key and management of other types of COMSEC material.

Source: CNSSI No. 4005 (COMSEC)

See key management infrastructure (KMI).

electronic messaging services

Services providing interpersonal messaging capability; meeting specific functional, management, and technical requirements; and yielding a business- quality electronic mail service suitable for the conduct of official government business.

electronic signature (C.F.D.)

See digital signature.

Rationale: Deprecated Term: Given that there is no current consensus on its definition, it is recommended that "digital signature" be used instead, if that context is what is intended.

electronically generated key

Key generated in a COMSEC device by introducing (either mechanically or electronically) a seed key into the device and then using the seed, together with a software algorithm stored in the device, to produce the desired key.

emission security (EMSEC)

The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from cryptoequipment and information systems. See TEMPEST.

Source: JP 6-0

embedded computer (C.F.D.)

Computer system that is an integral part of a larger system.

Rationale: Listed for deletion in 2010 version of CNSS 4009.

emergency action plan (EAP)

A plan developed to prevent loss of national intelligence; protect personnel, facilities, and communications; and recover operations damaged by terrorist attack, natural disaster, or similar events.

Source: ICS 700-01

encipher

See encrypt.

Rationale: Deprecated Term: Encrypt is the preferred term.

encryption certificate

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

Source: CNSSI No. 1300

enclave

A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

Source: IETF RFC 4949 Ver 2

enclave boundary

Point at which an enclave's internal network service layer connects to an external network's service layer, i.e., to another enclave or to a wide area network (WAN).

encode

Use a system of symbols to represent information, which might originally have some other representation. Example: Morse code.

Source: IETF RFC 4949 Ver 2

encrypt

Cryptographically transform data to produce cipher text.

Source: IETF RFC 4949 Ver 2

encrypted key

Key that has been encrypted in a system approved by the National Security Agency (NSA) for key encryption.

Source: CNSSI No. 4005 (COMSEC)

encryption

The cryptographic transformation of data to produce ciphertext.

Source: ISO/IEC 7498-2

encryption algorithm

Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key.

encryption certificate

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

Source: CNSSI No. 1300

end cryptographic unit (ECU)

Device that 1) performs cryptographic functions, 2) typically is part of a larger system for which the device provides security services, and 3) from the viewpoint of a supporting security infrastructure (e.g., a key management system) is the lowest level of identifiable component with which a management transaction can be conducted.

end-item accounting

Accounting for all the accountable components of a COMSEC equipment configuration by a single short title.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

end-to-end encryption

Communications encryption in which data is encrypted when being passed through a network, but routing information remains visible.

Source: NIST SP 800-12 (adapted)

end-to-end security

Safeguarding information in an information system from point of origin to point of destination.

enrollment manager

The management role that is responsible for assigning user identities to management and non-management roles.

enterprise

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

enterprise architecture (EA)

A strategic information asset base that defines the mission, the information necessary to perform the mission, the technologies necessary for performing the mission, and the transitional process for implementing new technologies in response to changing mission needs. The EA includes a baseline architecture, target architecture, and sequencing plan.

Source: CNSSP No. 24

enterprise cross domain services (ECDS)

A cross domain solution provided as a system across an enterprise infrastructure, fully integrated to provide the ability to access or transfer information between two or more security domains.

Source: CJCSI 6211.02D

enterprise cross domain services (ECDS) provider

An organization that establishes, manages and maintains the overall infrastructure and security posture offering automated capabilities to users and applications within an enterprise environment for information sharing across and among security domains.

Source: DoDI 8540.01

enterprise-hosted cross domain solutions

A point-to-point cross domain solution (CDS) that is managed by an enterprise cross domain service (ECDS) provider that may be available to additional users within the enterprise with little or no modifications.

Source: DoDI 8540.01

enterprise risk management

The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures as necessary.

enterprise service

A set of one or more computer applications and middleware systems hosted on computer hardware that provides standard information systems capabilities to end users and hosted mission applications and services.

environment of operation

The physical, technical, and organizational setting in which an information system operates, including but not limited to: missions/business functions; mission/business processes; threat space; vulnerabilities; enterprise and information security architectures; personnel; facilities; supply chain relationships; information technologies; organizational governance and culture; acquisition and procurement processes; organizational policies and procedures; organizational assumptions, constraints, risk tolerance, and priorities/trade-offs).

Source: NIST SP 800-30 Rev 1

erasure

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

Source: NIST SP 800-88 Rev 1

error detection code

A code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data.

Source: FIPS PUB 140-2

evaluated products list (EPL) (C.F.D.)

List of validated products that have been successfully evaluated under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS).

Rationale: EPL is no longer used. Product compliant list (PCL) is the replacement term.

evaluating authority

The official responsible for evaluating a reported COMSEC incident for the possibility of compromise.

Source: CNSSI No. 4006

evaluation assurance level (EAL) (C.F.D.)

Set of assurance requirements that represent a point on the Common Criteria predefined assurance scale.

Rationale: NIAP has switched to a “protection profile” program to secure devices.

event

Any observable occurrence in a network or system.

Source: NIST SP 800-61 Rev 2

examine

A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time.

Source: NIST SP 800-53A Rev 1

executive agency

An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

Source: 41 U.S.C. Sec. 403

exfiltration

The unauthorized transfer of information from an information system.

Source: NIST SP 800-53 Rev 4

expected output

Any data collected from monitoring and assessments as part of the information security continuous monitoring (ISCM) strategy.

Source: NIST SP 800-137

exploitable channel

Channel that allows the violation of the security policy governing an information system and is usable or detectable by subjects external to the trusted computing base. See covert channel.

eXtensible configuration checklist description format (XCCDF)

A language for authoring security checklists/benchmarks and for reporting results of evaluating them.

Source: NIST SP 800-126 Rev 2

external information system (or component)

An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

Source : NIST SP 800-37 Rev 1; NIST SP 800-53 Rev 4

external information system service

An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

Source: NIST SP 800-37 Rev 1; NIST SP 800-53 Rev 4

external information system service provider

A provider of external information system services to an organization through a variety of consumer-producer relationships, including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.

Source: NIST SP 800-37 Rev 1; NIST SP 800-53 Rev 4

external network

A network not controlled by the organization.

Source: NIST SP 800-53 Rev 4

external operational management role

A role intended to be performed by a manager who is typically a member of a key management infrastructure (KMI) customer organization.

Source: CNSSI No. 4005 (COMSEC)

extranet

A computer network that an organization uses for application data traffic between the organization and its business partners.

Source: IETF RFC 4949 Ver 2

fail safe

A mode of termination of system functions that prevents damage to specified system resources and system entities (i.e., specified data, property, and life) when a failure occurs or is detected in the system (but the failure still might cause a security compromise).

See fail secure and fail soft for comparison.

Source: IETF RFC 4949 Ver 2

fail secure

A mode of termination of system functions that prevents loss of secure state when a failure occurs or is detected in the system (but the failure still might cause damage to some system resource or system entity).

See fail safe and fail soft for comparison.

Source: IETF RFC 4949 Ver 2

fail soft

Selective termination of affected, non-essential system functions when a failure occurs or is detected in the system.

See fail safe and fail secure for comparison.

Source: IETF RFC 4949 Ver 2

failover

The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.

Source: NIST SP 800-53 Rev 4

failure access

Type of incident in which unauthorized access to data results from hardware or software failure.

failure control

Methodology used to detect imminent hardware or software failure and provide fail safe or fail soft recovery.

false acceptance

When a biometric system incorrectly identifies a biometric subject or incorrectly authenticates a biometric subject against a claimed identity.

Source: DoD Biometrics Enterprise Architecture (Integrated) v2.0

false accept rate (FAR)

Proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed.

Source: ISO/IEC 19795-1:2006

false rejection

The failure of a biometric system to identify a biometric subject or to verify the legitimate claimed identity of a biometric subject.

Source: NIAP 7298 (adapted); DoD Biometrics Enterprise Architecture (Integrated) v2.0

false reject rate (FRR)

Proportion of verification transactions with truthful claims of identity that are incorrectly denied.

Source: ISO/IEC 19795-1:2006

fault tree analysis

A top-down, deductive failure analysis in which an undesired state of a system (top event) is analyzed using Boolean logic to combine a series of lower-level events. An analytical approach whereby an undesired state of a system is specified and the system is then analyzed in the context of its environment of operation to find all realistic ways in which the undesired event (top event) can occur.

Source: NIST SP 800-30 Rev 1

federal agency

See executive agency.

Source: NIST SP 800-37 Rev 1

federal bridge certification authority (FBCA)

The Federal Bridge certification authority (CA) consists of a collection of public key infrastructure (PKI) components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer to peer interoperability among Agency Principal Certification Authorities.

Source: NIST SP 800-32

federal enterprise architecture (FEA)

A business-based framework that the Office of Management and Budget (OMB) developed for government-wide improvement in developing enterprise architectures (EAs) by providing a common framework to identify opportunities for simplifying processes and unifying work across the Federal Government.

Source: CNSSP No. 24

federal information processing standards (FIPS)

A standard for adoption and use by Federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.

Source: FIPS PUB 201-1

Federal Information Processing Standards (FIPS)-validated cryptography

A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP). See NSA-approved cryptography.

Source: NIST SP 800-53 Rev 4

Federal Information Security Management Act (FISMA)

Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Source: NIST SP 800-63-2

federal information system

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

Source: 40 U.S.C. Sec 11331

file protection

Aggregate of processes and procedures designed to inhibit unauthorized access, contamination, elimination, modification, or destruction of a file or any of its contents.

fill device

A COMSEC item used to transfer or store key in electronic form or to insert key into cryptographic equipment. The “Common Fill Devices” are the KYK-13, and KYK-15. Electronic fill devices include, but are not limited to, the DTD, SKL, SDS, and RASKI.

Source: CNSSI No. 4005 (COMSEC)

FIREFLY

Key management protocol based on public key cryptography.

FIREFLY credential manager

The key management entity (KME) responsible for removing outdated modern key credentials from the directory servers.

Source: CNSSI No. 4005 (COMSEC)

firewall

A gateway that limits access between networks in accordance with local security policy.

Source: NIST SP 800-32

firmware

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

Source: IETF RFC 4949 Ver 2

fixed COMSEC facility

COMSEC facility located in an immobile structure or aboard a ship.

Source: CNSSI No. 4005 (COMSEC)

flooding

An attack that attempts to cause a failure in a system by providing more input than the system can process properly.

Source: IETF RFC 4949 Ver 2

focused observation

The act of directed (focused) attention to a party or parties alleged to have violated Department/Agency (D/A) acceptable use' policies and agreements for NSS. The alleged violation may be caused by the aggregation of triggers indicating anomalous activity on a National Security System (NSS). The violation thresholds are arrived at by trigger events that meet established thresholds of anomalous activity or the observed violation of 'acceptable use' policies.

Source: CNSSD No. 504

focused testing

A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. Also known as gray box testing.

Source: NIST SP 800-53A Rev 1

forensic copy

An accurate bit-for-bit reproduction of the information contained on an electronic device or associated media, whose validity and integrity has been verified using an accepted algorithm.

Source: NIST SP 800-72

forensics

The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

formal access approval

A formalization of the security determination for authorizing access to a specific type of classified or controlled unclassified information (CUI) categories or subcategories based on specified access requirements, a determination of the individual's security eligibility, and a determination that the individual's official duties require the individual be provided access to the information.

Note: Providing access to, or transferring, CUI is based on Lawful Government Purpose unless such access is further restricted by law, regulation, or government wide policy.

formal method

Software engineering method used to specify, develop, and verify the software through application of a rigorous mathematically based notation and language.

Source: Guide to the Software Engineering Body of Knowledge

formal policy model

A description of specific behaviors or security policies using formal languages, thus enabling the correctness of those behaviors/policies to be formally proven.

Source: NIST SP 800-53 Rev 4 (adapted)

frequency hopping

Repeated switching of frequencies during radio transmission according to a specified algorithm, to minimize unauthorized interception or jamming of telecommunications.

full/depot maintenance (COMSEC)

Complete diagnostic repair, modification, and overhaul of COMSEC equipment, including repair of defective assemblies by piece part replacement. See limited maintenance.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

functional testing

Segment of quality assurance testing in which advertised security mechanisms of an information system are tested against a specification.

gateway

An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks.

Source: IETF RFC 4949 Ver 2

general support system (GSS)

An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

Source: OMB Circular A-130, App. III

global information grid (GIG) (C.F.D.)

The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG information technology (IT) includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network.

Source: JP 1-02

Rationale: Term has been replaced by the term “Department of Defense information networks (DODIN)”.

government off the shelf (GOTS)

A software and/or hardware product that is developed by the technical staff of a Government organization for use by the U.S. Government. GOTS software and hardware may be developed by an external entity, with specification from the Government organization to meet a specific Government purpose, and can normally be shared among Federal agencies without additional cost. GOTS products and systems are not commercially available to the general public. Sales and distribution of GOTS products and systems are controlled by the Government.

Source: NSA/CSS Policy 3-14

gray box testing

See focused testing.

gray market

Distribution channels which, while legal, are unofficial, unauthorized, or unintended by the original manufacturer.

Source: USDC DIB Assessment: Counterfeit Electronics (adapted)

group authenticator

Used, sometimes in addition to a sign-on authenticator, to allow access to specific data or functions that may be shared by all members of a particular group.

guard (system)

A computer system that (a) acts as gateway between two information systems operating under different security policies and (b) is trusted to mediate information data transfers between the two.

See transfer cross domain solution.

Source: IETF RFC 4949 Ver 2

hacker

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

hand receipt

A document used to record temporary transfer of COMSEC material from a COMSEC Account Manager to a user or maintenance facility and acceptance by the recipient of the responsibility for the proper storage, control, and accountability of the COMSEC material.

Source: CNSSI No. 4005 (COMSEC); NSA/CSS Manual Number 3-16 (COMSEC)

hand receipt holder

A user to whom COMSEC material has been issued a hand receipt. Known in EKMS and KMI as a Local Element.

Source: CNSSI No. 4005 (COMSEC)

handshake

Protocol dialogue between two systems for identifying and authenticating themselves to each other, or for synchronizing their operations with each other.

Source: IETF RFC 4949 Ver 2

hard copy key

Physical keying material, such as printed key lists, punched or printed key tapes, or programmable, read-only memories (PROMs).

Source: NSA/CSS Manual Number 3-16 (COMSEC)

hardware

The material physical components of an information system. See firmware and software.

Source: IETF RFC 4949 Ver 2

hardwired key

Key that is permanently installed.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

hash value/result

See message digest.

hash-based message authentication code (HMAC)

A message authentication code that uses a cryptographic key in conjunction with a hash function.

Source: FIPS PUB 201-1

hashing

The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.

Source: NIST SP 800-72

hashword (C.F.D.)

Memory address containing hash total.

Rationale: Listed for deletion in 2010 version of CNSS 4009.

High Assurance Internet Protocol Encryptor (HAIPE)

Device that provides networking, traffic protection, and management features that provide information assurance (IA) services in an IPv4/IPv6 network.

Source: CNSSP No. 19

High Assurance Internet Protocol Encryptor Interoperability Specification (HAIPE-IS)

Suite of documents containing the traffic protection, networking, and interoperability functional requirements necessary to ensure the interoperability of HAIPE compliant devices. This policy applies to HAIPE-IS Version 3.0.2 and all subsequent HAIPE-IS versions.

Source: CNSSP No. 19

high impact

The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e., 1) causes a severe degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2) results in major damage to organizational assets; 3) results in major financial loss; or 4) results in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.)

Source: FIPS PUB 199 (adapted)

high-impact system

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS PUB 199 potential impact value of high.

Note: For National Security Systems, CNSSI No. 1253 does not adopt this FIPS PUB 200 high water mark across security objectives.

Source: FIPS PUB 200

high-power transmitter

For the purposes of determining separation between RED equipment/lines and RF transmitters, high-power is that which exceeds 100 m Watt (20dBm) emitted isotropic radiated power (EIRP). See low-power transmitter.

Source: CNSSAM TEMPEST/01-13

honeypot

A system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders, like honey is attractive to bears.

Source: IETF RFC 4949 Ver 2

host

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

Source: CNSSI No. 1012, CNSSI No. 1013

host-based security

A set of capabilities that provide a framework to implement a wide-range of security solutions on hosts. This framework includes a trusted agent and a centralized management function that together provide automated protection to detect, respond, and report host-based vulnerabilities and incidents.

Source: CNSSI No. 1011

hot site

A fully operational offsite data processing facility equipped with hardware and software, to be used in the event of an information system disruption.

Source: NIST SP 800-34 Rev 1

hybrid security control

A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See common control and system-specific security control.

Source: NIST SP 800-37 Rev 1

IA architecture

A description of the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub- units, showing their alignment with the enterprise's mission and strategic plans.

Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially impact IA related terms.

IA infrastructure

The underlying security framework that lies beyond an enterprise's defined boundary, but supports its information assurance (IA) and IA-enabled products, its security posture and its risk management plan.

Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially impact IA related terms.

IA product

Product whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks.

Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially impact IA related terms.

IA-enabled information technology product (C.F.D.)

Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially impact IA related terms.

Rationale: Listed for deletion in 2010 version of CNSS 4009.

IA-enabled product

Product whose primary role is not security, but provides security services as an associated feature of its intended operating capabilities.

Note: Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security enabling messaging systems.

Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially impact IA related terms.

identification

The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.

Source: FIPS PUB 201-1

identifier

Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers.

Source: FIPS PUB 201-1

Note: This also encompasses non-person entities (NPEs).

identity

The set of physical and behavioral characteristics by which an individual is uniquely recognizable.

Source: FIPS PUB 201-1

Note: This also encompasses non-person entities (NPEs).

identity-based access control

Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity.

identity certificate

A certificate that provides authentication of the identity claimed. Within the National Security System (NSS) public key infrastructure (PKI), identity certificates may be used only for authentication or may be used for both authentication and digital signatures.

Source: CNSSI No. 1300

Identity, Credential, and Access Management (ICAM)

Programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and non-person entities (NPEs), bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency‘s resources.

See also attribute-based access control (ABAC).

Source: FICAM Roadmap and Implementation Guidance V2.0

identity registration

The process of making a person’s identity known to the personal identity verification (PIV) system, associating a unique identifier with that identity, and collecting and recording the person’s relevant attributes into the system.

Source: FIPS PUB 201-1

identity token

Smart card, metal key, or other physical object used to authenticate identity.

impact

The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.

Source: FIPS PUB 199 (adapted)

impact level

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Source: NIST SP 800-30 Rev 1

impact value

The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type, expressed as a value of low, moderate, or high.

Source: NIST SP 800-30 Rev 1

implant

Electronic device or electronic equipment modification designed to gain unauthorized interception of information-bearing emanations.

inadvertent disclosure

Type of incident involving accidental exposure of information to an individual not authorized access.

incident

An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. See cyber incident. See also event, security-relevant, and intrusion.

Source: FIPS PUB 200 (adapted)

incident handling

The mitigation of violations of security policies and recommended practices.

Source: NIST SP 800-61 Rev 2

incident response

See incident handling.

incident response plan

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information systems(s).

Source: NIST SP 800-34 Rev 1

independent validation authority (IVA)

Entity that reviews the soundness of independent tests and system compliance with all stated security controls and risk mitigation actions. IVAs will be designated by the authorizing official as needed.

independent verification & validation (IV&V)

A comprehensive review, analysis, and testing, (software and/or hardware) performed by an objective third party to confirm (i.e., verify) that the requirements are correctly defined, and to confirm (i.e., validate) that the system correctly implements the required functionality and security requirements.

indicator

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

individuals

An assessment object that includes people applying specifications, mechanisms, or activities.

Source: NIST SP 800-39

individual accountability

Ability to associate positively the identity of a user with the time, method, and degree of access to an information system.

industrial control system (ICS)

General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

Source: NIST SP 800-82 Rev 1

information

1. Facts and ideas, which can be represented (encoded) as various forms of data.

2. Knowledge -- e.g., data, instructions -- in any medium or form that can be communicated between system entities.

Source: IETF RFC 4949 Ver 2

information and communications technology (ICT)

Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).

Source: DoDI 5200.44

information assurance (IA)

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

Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially impact IA related terms.

information assurance (IA) professional (C.F.D.)

Individual who works IA issues and has real world experience plus appropriate IA training and education commensurate with their level of IA responsibility.

Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially impact IA related terms.

Rationale: Term is self-describing and generic.

information assurance component (IAC)

An application (hardware and/or software) that provides one or more Information Assurance capabilities in support of the overall security and operational objectives of a system.

Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially impact IA related terms.

information assurance manager (IAM) (C.F.D.)

See information systems security manager (ISSM).

Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially impact IA related terms.

Rationale: Term is deprecated in favor of ISSM.

information assurance officer (IAO) (C.F.D.)

See information systems security officer (ISSO).

Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially impact IA related terms.

Rationale: Term is deprecated in favor of ISSO.

information assurance vulnerability alert (IAVA)

Notification that is generated when an Information Assurance vulnerability may result in an immediate and potentially severe threat to DoD systems and information; this alert requires corrective action because of the severity of the vulnerability risk.

Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially impact IA related terms.

information assurance vulnerability bulletin (IAVB)

Addresses new vulnerabilities that do not pose an immediate risk to DoD systems, but are significant enough that noncompliance with the corrective action could escalate the risk.

Source: SECNAV M-5239.1 (adapted)

Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially impact IA related terms.

information domain

A three-part concept for information sharing, independent of, and across information systems and security domains that 1) identifies information sharing participants as individual members, 2) contains shared information objects, and 3) provides a security policy that identifies the roles and privileges of the members and the protections required for the information objects.

information environment

The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

Source: JP 3-13

information flow control

Procedure to ensure that information transfers within an information system are not made in violation of the security policy.

information management

The planning, budgeting, manipulating, and controlling of information throughout its life cycle.

information operations (IO)

The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called IO.

Source: DoD JP 3-13

information owner

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal. See information steward.

Source: FIPS PUB 200

Note: Information steward is a related term, but it is not identical to information owner.

information resources

Information and related resources, such as personnel, equipment, funds, and information technology.

Source: 44 U.S.C. SEC. 3502

information resources management (IRM)

The planning, budgeting, organizing, directing, training, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by agencies.

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.

Source: 44 U.S.C. Sec 3542

information security architect

Individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes.

Source: NIST SP 800-37 Rev 1

information security continuous monitoring (ISCM)

Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Note: The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.

See organizational information security continuous monitoring and automated security monitoring.

Source: NIST SP 800-137

information security continuous monitoring (ISCM) process

A process to:

- Define an ISCM strategy;
- Establish an ISCM program;
- Implement an ISCM program;
- Analyze data and Report findings;
- Respond to findings; and
- Review and Update the ISCM strategy and program.

Source: NIST SP 800-137

information security continuous monitoring (ISCM) program

A program established to collect information in accordance with pre-established metrics, utilizing information readily available in part through implemented security controls.

Source: NIST SP 800-137

information security policy

Aggregate of directives, regulations, and rules that prescribe how an organization manages, protects, and distributes information.

information security program plan

Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.

Source: NIST SP 800-37 Rev 1

information security risk

The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. See risk.

Source: NIST SP 800-30 Rev 1

information sharing environment (ISE)

1. An approach that facilitates the sharing of terrorism and homeland security information.

2. ISE in its broader application enables those in a trusted partnership to share, discover, and access controlled information.

information steward

Individual or group that helps to ensure the careful and responsible management of federal information belonging to the Nation as a whole, regardless of the entity or source that may have originated, created, or compiled the information. Information stewards provide maximum access to federal information to elements of the federal government and its customers, balanced by the obligation to protect the information in accordance with the provisions of the Federal Information Security Management Act (FISMA) and any associated security-related federal policies, directives, regulations, standards, and guidance.

Source: NIST SP 800-37 Rev 1

information system (IS)

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

Source: 44 U.S.C. Sec 3502

Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

information system boundary

See authorization boundary.

Source: NIST SP 800-37 Rev 1

information system component

A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products.

Source: NIST SP 800-53 Rev 4

information system life cycle

The phases through which an information system passes, typically characterized as initiation, development, operation, and termination (i.e., sanitization, disposal and/or destruction).

information system owner (or program manager)

Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Source: NIST SP 800-37 Rev 1; NIST SP 800-53 Rev 4 information system resilience

The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.

Source: NIST SP 800-39

information system-related security risks

Risk that arises through the loss of confidentiality, integrity, or availability of information or information systems considering impacts to organizational operations and assets, individuals, other organizations, and the Nation. A subset of information security risk. See risk.

Source: NIST SP 800-30 Rev 1

information system service

A capability provided by an information system that facilitates information processing, storage, or transmission.

Source: NIST SP 800-53 Rev 4

information systems security (INFOSEC)

The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. See information assurance (IA).

Source: NSA/CSS Manual Number 3-16 (COMSEC)

information systems security (INFOSEC) boundary

An imaginary definable perimeter encompassing all the critical functions in an INFOSEC product and separating them from all other functions within the product.

Note: INFOSEC Boundary is in terms of a product assessment; not to be confused with authorization boundary.

Source: NSA Information Assurance Security Requirements Directive (IASRD) dated October, 2012

information systems security engineer (ISSE)

Individual assigned responsibility for conducting information system security engineering activities.

Source: NIST SP 800-37 Rev 1

information systems security engineering (ISSE)

Process that captures and refines information security requirements and ensures their integration into information technology component products and information systems through purposeful security design or configuration.

Source: NIST SP 800-37 Rev 1

information systems security manager (ISSM)

Individual responsible for the information assurance of a program, organization, system, or enclave.

information system security officer (ISSO)

Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program.

Source: NIST SP 800-30 Rev 1

information technology (IT)

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Source: 40 U.S.C. Sec. 11101 (adapted); 40 U.S.C. Sec. 1401 (adapted)

information technology product

See information system component.

information type

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or in some instances, by a specific law, Executive Order (E.O.), directive, policy, or regulation.

Source: FIPS PUB 199

information value

A qualitative measure of the importance of the information based upon factors such as the level of robustness of the information assurance (IA) controls allocated to the protection of information based upon: mission criticality, the sensitivity (e.g., classification and compartmentalization) of the information, releasability to other countries, perishability/longevity of the information (e.g., short life data versus long life intelligence source data), and potential impact of loss of confidentiality and integrity and/or availability of the information.

inheritance

See security control inheritance.

insider

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

Source: CNSSD No. 504

insider threat

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

Source: CNSSD No. 504 (adapted)

insider threat program

A coordinated collection of capabilities authorized by the Department/Agency (D/A) that is organized to deter, detect, and mitigate the unauthorized disclosure of sensitive information.

Source: CNSSD No. 504

inspectable space

Three dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and remove a potential TEMPEST exploitation exists. Synonymous with zone of control.

Source: CNSSAM TEMPEST/01-13 (adapted)

integrated CCI (controlled cryptographic items) component

A CCI component that is designed to be incorporated into an otherwise unclassified communication or information processing equipment or system to form a CCI equipment or CCI system.

Note: The integrated CCI component cannot perform any function by itself. It obtains power from the host equipment. An integrated CCI component may take a variety of forms (see paragraph 8 of the basic Instruction regarding the terminology for CCI component).

Source: CNSSI No. 4001

integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Source: 44 U.S.C. Sec. 3542

integrity check value (C.F.D.)

See checksum.

Rationale: The concept of an integrity check value is included in the term "checksum." As such, it is not necessary to distinguish between the two terms.

intellectual property

Creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract “properties” has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered.

intelligence

1.
a. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.
b. The activities that result in the product.
c. The organizations engaged in such activities.

Source: Joint Publication 2-0

2. The term 'intelligence' includes foreign intelligence and counterintelligence.

Source: 50 U.S.C. Sec. 3003

intelligence activities

All activities that agencies within the Intelligence Community are authorized to conduct pursuant to Executive Order (E.O.) 12333, United States Intelligence Activities.

Source: E.O. 12333

intelligence community (IC)

Intelligence Community and elements of the Intelligence Community refers to:

(1) The Office of the Director of National Intelligence;
(2) The Central Intelligence Agency;
(3) The National Security Agency;
(4) The Defense Intelligence Agency;
(5) The National Geospatial-Intelligence Agency;
(6) The National Reconnaissance Office;
(7) The other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;
(8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;
(9) The intelligence elements of the Federal Bureau of Investigation;
(10) The Office of National Security Intelligence of the Drug Enforcement Administration;
(11) The Office of Intelligence and Counterintelligence of the Department of Energy;
(12) The Bureau of Intelligence and Research of the Department of State;
(13) The Office of Intelligence and Analysis of the Department of the Treasury;
(14) The Office of Intelligence and Analysis of the Department of Homeland Security;
(15) The intelligence and counterintelligence elements of the Coast Guard; and
(16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community.

Source: E.O. 12333 (As amended by E.O.s 13284 (2003), 13355 (2004) and 13470 (2008))

interconnection security agreement (ISA)

A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high- level roles and responsibilities in management of a cross-domain connection.

interface

Common boundary between independent systems or modules where interactions take place.

interim approval to operate (IATO) (C.F.D.)

Temporary authorization granted by principal accrediting authority (PAA) or authorizing official (AO) for an information system to process information based on preliminary results of a security evaluation of the system. (To be replaced by ATO and plan of action and milestones (POA&M))

Rationale: Term has been replaced by the term “authorization to operate (ATO)” with conditions.

interim authorization to test (IATT)

Temporary authorization to test an information system in a specified operational information environment within the timeframe and under the conditions or constraints enumerated in the written authorization.

Intermediate Certification Authority (CA)

A CA that is signed by a superior CA (e.g., a Root CA or another Intermediate CA) and signs CAs (e.g., another Intermediate or Subordinate CA). The Intermediate CA exists in the middle of a trust chain between the Trust Anchor, or Root, and the subscriber certificate issuing Subordinate CAs.

Source: CNSSI No. 1300

internal network

A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology provides the same effect. An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.

Source: NIST SP 800-53 Rev 4

internal security controls

Hardware, firmware, or software features within an information system that restrict access to resources to only authorized subjects.

Internet

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

Source: IETF RFC 4949 Ver 2

internet protocol (IP)

Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.

interview

A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control effectiveness over time.

Source: NIST SP 800-53A Rev 1

intranet

A computer network, especially one based on Internet technology, that an organization uses for its own internal (and usually private) purposes and that is closed to outsiders.

Source: IETF RFC 4949 Ver 2

intrusion

A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so.

Source: IETF RFC 4949 Ver 2

intrusion detection

The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents.

Source: NIST SP 800-94

intrusion detection system (IDS)

Software that automates the intrusion detection process.

Source: NIST SP 800-94

intrusion detection system (IDS), (host-based)

IDSs which operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the Operating System. Furthermore, unlike network-based IDSs, host- based IDSs can more readily “see” the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks.

Source: NIST SP 800-36

intrusion detection systems (IDS), (network-based)

IDSs which detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment.

Source: NIST SP 800-36

intrusion prevention

The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents.

Source: NIST SP 800-94

intrusion prevention system (IPS)

Intrusion Prevention System: Software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Source: NIST SP 800-94

IP security (IPSec)

Provide(s) interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, detection and rejection of replays (a form of partial sequence integrity), confidentiality (via encryption), and limited traffic flow confidentiality.

Source: IETF RFC 4301

IT security awareness and training program

Explains proper rules of behavior for the use of agency information systems and information. The program communicates information technology (IT) security policies and procedures that need to be followed. (i.e., NSTISSD 501, NIST SP 800-50)

inventory

(a) The physical or virtual verification of the presence of each item of COMSEC material charged to a COMSEC account.

(b) A listing of each item of material charged to a COMSEC account.

Source: CNSSI No. 4005 (COMSEC)

jamming

An attack that attempts to interfere with the reception of broadcast communications.

Source: IETF RFC 4949 Ver 2

joint authorization

Security authorization involving multiple authorizing officials.

Source: NIST SP 800-37 Rev 1

key

A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. Usually a sequence of random or pseudorandom bits used initially to set up and periodically change the operations performed in cryptographic equipment for the purpose of encrypting or decrypting electronic signals, or for determining electronic counter-countermeasures (ECCM) patterns, or for producing other key.

Source: CNSSI No. 4005 (COMSEC)

key administration

Functions of loading, storing, copying, and distributing the keys and producing the necessary audit information to support those functions. (System Unique).

Source: NSTISSI No. 3006

key agreement

A key-establishment procedure where resultant keying material is a function of information contributed by two or more participants, so that no party can predetermine the value of the keying material independently of the other party's contribution.

Source: NIST SP 800-57 Part 1 Rev 3

key distribution

The transport of a key and other keying material from an entity that either owns or generates the key to another entity that is intended to use the key.

Source: NIST SP 800-57 Part 1 Rev 3

key distribution center (KDC)

COMSEC facility generating and distributing key in electronic form.

key encryption key (KEK)

A key that encrypts other key (typically traffic encryption keys (TEKs)) for transmission or storage.

Source: CNSSI No. 4005 (COMSEC)

key escrow

The retention of the private component of the key pair associated with a subscriber's encryption certificate to support key recovery.

Source: CNSSI No. 1300

key escrow system

The system responsible for storing and providing a mechanism for obtaining copies of private keys associated with encryption certificates, which are necessary for the recovery of encrypted data.

Source: CNSSI No. 1300

key establishment

A function in the lifecycle of keying material; the process by which cryptographic keys are securely established among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key-transport and/or key-agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement).

Source: NIST SP 800-57 Part 1 Rev 3

key exchange

Process of exchanging public keys (and other information) in order to establish secure communications.

Note: See related term “key transport”.

Source: NIST SP 800-32 (adapted)

key generation material

Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.

Source: NIST SP 800-32

key list

A printed series of key settings for a specific cryptonet. Key lists may be produced in list, pad, or printed tape format.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

key loader

A self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.

Source: FIPS PUB 140-2

key management

The activities involving the handling of cryptographic keys and other related security parameters (e.g. passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction.

Source: NIST SP 800-57 Part 1 Rev 3

key management device

A unit that provides for secure electronic distribution of encryption keys to authorized users.

key management entity (KME)

Any activity/organization that performs key management related functionality and has been assigned an electronic key management system (EKMS) ID.

Source: CNSSI No. 4005 (COMSEC)

key management infrastructure (KMI)

The framework and services that provide the generation, production, storage, protection, distribution, control, tracking, and destruction for all cryptographic keying material, symmetric keys as well as public keys and public key certificates.

Source: CNSSI No. 4005 (COMSEC)

key pair

A public key and its corresponding private key; a key pair is used with a public key algorithm.

Source: NIST SP 800-57 Part 1 Rev 3

key processor (KP)

The high-assurance cryptographic component in electronic key management system (EKMS) designed to provide for the local generation of keying material, encryption, and decryption of key, key load into electronic fill devices, and message signature functions.

Source: CNSSI No. 4005 (COMSEC)

key recovery

A function in the lifecycle of keying material; mechanisms and processes that allow authorized entities to retrieve or reconstruct keying material from key backup or archive.

Source: NIST SP 800-57 Part 1 Rev 3

key stream

Sequence of symbols (or their electrical or mechanical equivalents) produced in a machine or auto-manual cryptosystem to combine with plain text to produce cipher text, control transmission security processes, or produce key.

key tag

Identification information associated with certain types of electronic key.

key tape

Punched or magnetic tape containing key. Printed key in tape form is referred to as a key list.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

key transport

A key-establishment procedure whereby one party (the sender) selects and encrypts the keying material and then distributes the material to another party (the receiver).

When used in conjunction with a public-key (asymmetric) algorithm, the keying material is encrypted using the public key of the receiver and subsequently decrypted using the private key of the receiver. When used in conjunction with a symmetric algorithm, the keying material is encrypted with a key-encrypting key shared by the two parties.

Source: NIST SP 800-57 Part 1 Rev 3

key update

A function performed on a cryptographic key in order to compute a new, but related, key.

Source: NIST SP 800-57 Part 1 Rev 3

Key-Auto-Key (KAK)

Cryptographic logic using previous key to produce key.

keyed hash-based message authentication code (HMAC)

A message authentication code that uses a cryptographic key in conjunction with a hash function.

Source: FIPS PUB 198-1

Key-Encryption-Key (KEK)

A key that encrypts other key (typically Traffic Encryption Keys or TEKs) for transmission or storage.

Source: CNSSI No. 4005 (COMSEC)

keying material

Key, code, or authentication information in physical, electronic, or magnetic form. It includes key tapes and list, codes, authenticators, one-time pads, floppy disks, and magnetic tapes containing keys, plugs, keyed microcircuits, electronically generated key, etc.

Source: CNSSI No. 4005 (COMSEC)

keystroke monitoring

The process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails.

Source: NIST SP 800-12

KMI operating account (KOA)

A key management infrastructure (KMI) business relationship that is established 1) to manage the set of user devices that are under the control of a specific KMI customer organization; and 2) to control the distribution of KMI products to those devices.

KMI protected channel (KPC)

A key management infrastructure (KMI) Communication Channel that provides 1) Information Integrity Service; 2) either Data Origin Authentication Service or Peer Entity Authentication Service, as is appropriate to the mode of communications; and 3) optionally, Information Confidentiality Service.

KMI-aware device

A user device that has a user identity for which the registration has significance across the entire key management infrastructure (KMI) (i.e., the identity's registration data is maintained in a database at the primary services node (PRSN) level of the system, rather than only at an MGC) and for which a product can be generated and wrapped by a product source node (PSN) for distribution to the specific device.

KOA agent

A user identity that is designated by a key management infrastructure operating account (KOA) manager to access primary services node (PRSN) product delivery enclaves for the purpose of retrieving wrapped products that have been ordered for user devices that are assigned to that KOA.

KOA manager (KOAM)

An external operational management role that is responsible for the operation of a key management infrastructure operating account (KOA) that includes all distribution of KMI key and products from the management client (MGC) to the end cryptographic units (ECUs) and fill devices, and management and accountability of all electronic and physical key, and physical COMSEC materials from receipt and/or production to destruction or transfer to another KOA. (Similar to an electronic key management system (EKMS) Manager or COMSEC Account Manager)

Source: CNSSI No. 4005 (COMSEC)

KOA registration manager

The individual responsible for performing activities related to registering key management infrastructure operating accounts (KOAs).

label

See security label.

labeled security protections

Access control protection features of a system that use security labels to make access control decisions.

laboratory attack (C.F.D.)

Use of sophisticated signal recovery equipment in a laboratory environment to recover information from data storage media.

Source: NIST SP 800-88 Rev 1 (adapted)

Rationale: Term is no longer used in revised version of NIST SP 800-88.

lawful government purpose

Any activity, function, operation, or other circumstance the Government authorizes; also the standard to apply when determining whether individuals, organizations, or groups of users may receive or access controlled unclassified information (CUI) that is not subject to a limited dissemination control authorized by the CUI Executive Agent.

Source: 32 CFR 2002 (draft)

layered COTS product solutions

Commercial information assurance (IA) and IA-enabled information technology (IT) components used in layered solutions approved by the National Security Agency (NSA) to protect information carried on national security systems (NSSs).

See commercial solutions for classified.

Source: CNSSP No. 11

least privilege

The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

least trust

The principle that a security architecture should be designed in a way that minimizes 1) the number of components that require trust; and 2) the extent to which each component is trusted.

likelihood of occurrence

A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.

Source: NIST SP 800-30 Rev 1

limited maintenance (COMSEC)

COMSEC maintenance restricted to fault isolation, removal, and replacement of plug-in assemblies. Soldering or unsoldering usually is prohibited in limited maintenance. See full maintenance.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

line conditioning

Elimination of unintentional signals or noise induced or conducted on a telecommunications or information system signal, power, control, indicator, or other external interface line.

line conduction

Unintentional signals or noise induced or conducted on a telecommunications or information system signal, power, control, indicator, or other external interface line.

link encryption

Encryption of information between nodes of a communications system.

line of business

The following Office of Management and Budget (OMB)-defined process areas common to virtually all federal agencies: Case Management, Financial Management, Grants Management, Human Resources Management, Federal Health Architecture, Information Systems Security, Budget Formulation and Execution, Geospatial, and information technology (IT) Infrastructure.

Source: NIST SP 800-53 Rev 4

local access

Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

Source: NIST SP 800-53 Rev 4

local authority

Organization responsible for generating and signing user certificates in a public key infrastructure (PKI)-enabled environment.

local COMSEC management software (LCMS)

Application-level software on the local management device (LMD) that provides for the management of key, physical COMSEC materials, non-cryptographic services, and communications. Through a graphical interface, the LCMS automates the functions of the COMSEC Account Manager, including accounting, auditing, distribution, ordering, and production. Programs and systems that have specialized key management requirements have software shell programs (known as user applications software (UAS)) that run on the LMD with the LCMS software to provide custom functionality.

Source: CNSSI No. 4005 (COMSEC)

local element

See hand receipt holder.

Source: CNSSI No. 4005 (COMSEC)

local management device (LMD)

The component in electronic key management system (EKMS) that provides electronic management of key and other COMSEC material and serves as an interface to the Key Processor. (It is composed of a user-supplied personal computer, an operating system, LCMS and user application software (UAS), as required).

Source: CNSSI No. 4005 (COMSEC)

local registration authority (LRA)

A registration authority with responsibility for a local community.

Source: NIST SP 800-32

logic bomb

A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

logical access control system

An automated system that controls an individual's ability to access one or more computer system resources such as a workstation, network, application, or database. A logical access control system requires validation of an individual's identity through some mechanism such as a personal identification number (PIN), card, biometric, or other token. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

Source: NIST SP 800-53 Rev 4

logical perimeter

A conceptual perimeter that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system without a reliable human review by an appropriate authority. The location of such a review is commonly referred to as an "air gap".

long title

The descriptive title of a COMSEC item.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

low impact

The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e., 1) causes a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; 2) results in minor damage to organizational assets; 3) results in minor financial loss; or 4) results in minor harm to individuals).

Source: FIPS PUB 200 (adapted)

low probability of detection (LPD)

Result of measures used to hide or disguise intentional electromagnetic transmissions.

Source: CNSSI No. 1200 (adapted)

low probability of intercept (LPI)

Result of measures used to resist attempts by adversaries to analyze the parameters of a transmission to determine if it is a signal of interest.

Source: CNSSI No. 1200

low probability of positioning

Result of measures used to resist attempts by adversaries to determine the location of a particular transmitter.

Source: CNSSI No. 1200

low-impact system

An information system in which all three security properties (i.e., confidentiality, integrity, and availability) are assigned a FIPS PUB 199 potential impact value of low.

Note: For National Security Systems, CNSSI No. 1253 does not adopt this FIPS PUB 200 high water mark across security objectives.

Source: FIPS PUB 200

low-power transmitter

For the purposes of determining separation between RED equipment/lines and radio frequency (RF) transmitters, low-power is that which is less than or equal to 100 m Watt (20 dBm) effective isotropic radiated power (EIRP). Examples of low-power transmitters are wireless devices for local communications that do not need a Federal Communications Commission (FCC) license, such as some IEEE 802.11X network access points, and portable (but not cellular) telephones.

Source: CNSSAM TEMPEST/01-13

macro virus

A virus that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate.

magnetic remanence

Magnetic representation of residual information remaining on a magnetic medium after the medium has been cleared. See clearing.

maintenance key

Key intended only for off-the-air, in-shop use. Maintenance key may not be used to protect classified or sensitive U.S. Government information. Also known as bench test key.

Source: CNSSI No. 4005 (COMSEC)

major application

An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

Source: OMB Circular A-130 (adapted)

malicious code

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Source: NIST SP 800-53 Rev 4

malicious cyber activity

Activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

Source: PPD 20

malicious logic

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

Source: IETF RFC 4949 Ver 2

malware

See malicious code and malicious logic.

managed interface

An interface within an information system that provides boundary protection capability using automated mechanisms or devices.

Source: NIST SP 800-53 Rev 4

management client (MGC)

A configuration of a client node that enables a key management infrastructure (KMI) external operational manager to manage KMI products and services by either 1) accessing a PRSN or 2) exercising locally-provided capabilities. A management client (MGC) consists of a client platform and an advanced key processor (AKP).

management controls (C.F.D.)

The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

Source: FIPS PUB 200

Rationale: Listed for deletion in 2010 version of CNSS 4009.

management security controls (C.F.D.)

The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information systems security.

Rationale: Listed for deletion in 2010 version of CNSS 4009.

mandatory access control (MAC)

An access control policy that is uniformly enforced across all subjects and objects within the boundary of an information system. A subject that has been granted access to information is constrained from doing any of the following: (i) passing the information to unauthorized subjects or objects; (ii) granting its privileges to other subjects; (iii) changing one or more security attributes on subjects, objects, the information system, or system components; (iv) choosing the security attributes to be associated with newly-created or modified objects; or (v) changing the rules governing access control. Organization-defined subjects may explicitly be granted organization-defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all of the above constraints.

Source: NIST SP 800-53 Rev 4

mandatory modification (MAN)

A change to a COMSEC end-item, which the National Security Agency (NSA) requires to be completed and reported by a specified date. See optional modification.

Source: NSA/CSS Manual Number 3-16 (COMSEC) (adapted)

man-in-the-middle attack (MitM)

A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.

Source: IETF RFC 4949 Ver 2

manipulative communications deception (C.F.D.)

Alteration or simulation of friendly telecommunications for the purpose of deception. See communications deception and imitative communications deception.

Rationale: Listed for deletion in 2010 version of CNSS 4009.

manual cryptosystem

Cryptosystem in which the cryptographic processes are performed without the use of crypto-equipment or auto-manual devices.

manual remote rekeying

Procedure by which a distant crypto-equipment is rekeyed electronically, with specific actions required by the receiving terminal operator. Synonymous with cooperative remote rekeying. See automatic remote rekeying.

marking

See security marking.

masquerading

A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity.

match/matching

The process of comparing biometric information against a previously stored template(s) and scoring the level of similarity.

Source: FIPS PUB 201-1

mechanisms

An assessment object that includes specific protection-related items (e.g., hardware, software, or firmware) employed within or at the boundary of an information system.

Source: NIST SP 800-53A Rev 1

media

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

Source: FIPS PUB 200

media sanitization

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

Source: NIST SP 800-88 Rev 1

memorandum of agreement (MOA)

A type of intra-agency, interagency, or National Guard agreement between two or more parties, which includes specific terms that are agreed to, and a commitment by at least one party to engage in action. It includes either a commitment of resources or binds a party to a specific action.

Source: DoDI 4000.19

memorandum of understanding (MOU)

A type of intra-agency, interagency, or National Guard agreement between two or more parties, which includes only general understandings between the parties. It neither includes a commitment of resources nor binds a party to a specific action.

Source: DoDI 4000.19

memory scavenging

The collection of residual information from data storage.

message authentication code (MAC)

A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.

See checksum.

Source: FIPS PUB 201-1

message digest

The result of applying a hash function to a message. Also known as a “hash value” or “hash output”.

Source: NIST SP 800-107 Rev 1

message indicator (MI)

Sequence of bits transmitted over a communications system for synchronizing cryptographic equipment.

metadata

Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).

Source: NIST SP 800-53 Rev 4

metrics

Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.

Source: NIST SP 800-55

minor application

An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.

Source: NIST SP 800-18 Rev 1

misnamed files

A technique used to disguise a file’s content by changing the file’s name to something innocuous or altering its extension to a different type of file, forcing the examiner to identify the files by file signature versus file extension.

Source: NIST SP 800-72

mission assurance category (MAC) (C.F.D.)

A Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) term primarily used to determine the requirements for availability and integrity.

Rationale: The Risk Management Framework updates the method for determining the potential impact due to the loss of integrity and availability, which is what the MAC covered. These security objectives are treated independently under system categorization IAW CNSSI No. 1253.

mission/business segment

Elements of organizations describing mission areas, common/shared business services, and organization-wide services. Mission/business segments can be identified with one or more information systems which collectively support a mission/business process.

Source: NIST SP 800-30 Rev 1

mission critical

Any telecommunications or information system that is defined as a national security system (Federal Information Security Management Act (FISMA) of 2002) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.

Source: NIST SP 800-60 Vol 1 Rev 1

mission-critical element

A system component or subsystem that delivers mission critical functionality to a system or that may, by virtue of system design, introduce vulnerability to mission critical functions.

Note: Mission-critical element is often denoted as "critical component".

Source: CNSSD No. 505

mission-critical functionality

Any system function, the compromise of which would degrade the effectiveness of that system in achieving the core mission for which it was designed.

Source: CNSSD No. 505

misuse of Controlled Unclassified Information (CUI)

Any situation where controlled unclassified information (CUI) is used in a manner inconsistent with the policy contained in Executive Order 13556, 32 Code of Federal Regulations (CFR), the CUI Registry, additional issuances from the CUI Executive Agent, or any of the laws, regulations, and Government-wide policies that establish the designation of CUI categories and subcategories. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI.

Source: 32 CFR 2002 (draft)

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.

Source: NIST SP 800-53 Rev 4

Note: Some examples of software technologies that provide the mechanisms for the production and use of mobile code include Java, JavaScript, ActiveX, VBScript, etc.

mobile code risk categories

Categories of risk associated with mobile code technology based on functionality, level of access to workstation, server, and remote system services and resources, and the resulting threat to information systems.

Source: DoDI 8500.01

mobile code technologies

Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).

Source: NIST SP 800-53 Rev 4

mobile device

A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers.

Source: NIST SP 800-53 Rev 4

Note: If the device only has storage capability and is not capable of processing or transmitting/receiving information, then it is considered a portable storage device, not a mobile device. See portable storage device.

moderate-impact

The loss of confidentiality, integrity, or availability that could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e., 1) causes a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2) results in significant damage to organizational assets; 3) results in significant financial loss; or 4) results in significant harm to individuals that does not involve loss of life or serious life threatening injuries.).

Source: FIPS PUB 200 (adapted)

moderate-impact system

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS PUB 199 potential impact value of moderate and no security objective is assigned a FIPS PUB 199 potential impact value of high.

Note: For National Security Systems, CNSSI No. 1253 does not adopt this FIPS PUB 200 high water mark across security objectives.

Source: FIPS PUB 200

modern key

A collective name for asymmetric key such as secure data network system (SDNS) FIREFLY key and message signature key. It does not include the public key infrastructure (PKI) system or keys.

Source: CNSSI No. 4006

multifactor authentication

Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See authenticator.

Source: NIST SP 800-53 Rev 4

multilevel device

Equipment trusted to properly maintain and separate data of different security domains.

multi-level cross domain solution

A type of cross domain solution (CDS) that uses trusted labeling to store data at different classifications and allows users to access the data based upon their security domain and credentials.

Source: CNSSI No. 1253F Attachment 3 (adapted)

multi-level security (MLS)

Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization.

multi-level solution

Store data in multiple security domains at varied security levels and allow users to access the data at an appropriate security level.

Source: DoDI 8540.01

multiple security levels (MSL)

Capability of an information system that is trusted to contain, and maintain separation between, resources (particularly stored data) of different security domains.

multi-releasable

A characteristic of an information domain where access control mechanisms enforce policy-based release of information to authorized users within the information domain.

mutual authentication

The process of both entities involved in a transaction verifying each other.

National COMSEC Incident Reporting System (NCIRS)

System established by the National Security Agency (NSA) as a means of ensuring that all reported incidents are evaluated so that actions can be taken to minimize any adverse impact on national security. The NCIRS is comprised of the organizations within the NSS community (NSA, heads of Department or Agency, material controlling authorities, and product resource managers) responsible for the reporting and evaluation of COMSEC incidents.

Source: CNSSI No. 4003

National Information Assurance Partnership (NIAP)

A U.S. Government initiative established to promote the use of evaluated information systems products and champion the development and use of national and international standards for information technology security. NIAP was originally established as collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in fulfilling their respective responsibilities under P.L. 100-235 (Computer Security Act of 1987). NIST officially withdrew from the partnership in 2007 but NSA continues to manage and operate the program. The key operational component of NIAP is the Common Criteria Evaluation and Validation Scheme (CCEVS) which is the only U.S. Government- sponsored and endorsed program for conducting internationally-recognized security evaluations of commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled information technology products. NIAP employs the CCEVS to provide government oversight or “validation” to U.S. Common Criteria (CC) evaluations to ensure correct conformance to the International Common Criteria for IT Security Evaluation (ISO/IEC 15408).

national information infrastructure (NII)

Nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. It includes both public and private networks, the internet, the public switched network, and cable, wireless, and satellite communications.

national security emergency preparedness telecommunications services

Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.

Source: 47 CFR Part 64 Appendix A

national security information (NSI)

See classified national security information.

national security system (NSS)

(A) Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—
(i) the function, operation, or use of which—
(I) involves intelligence activities;
(II) involves cryptologic activities related to national security;
(III) involves command and control of military forces;
(IV) involves equipment that is an integral part of a weapon or weapons system; or
(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or
(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A) (i) (V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Source: 44 U.S.C. SEC 3542 (b)(2)

national vulnerability database (NVD)

The U.S. Government repository of standards based vulnerability management data, enabling automation of vulnerability management, security measurement, and compliance (e.g., FISMA).

Source: http://nvd.nist.gov/

need-to-know

A determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Source: E.O. 13526

need-to-know determination

Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties.

net-centric architecture

A complex system of systems composed of subsystems and services that are part of a continuously evolving, complex community of people, devices, information and services interconnected by a network that enhances information sharing and collaboration. Subsystems and services may or may not be developed or owned by the same entity, and, in general, will not be continually present during the full life cycle of the system of systems. Examples of this architecture include service-oriented architectures and cloud computing architectures.

Source: NIST SP 800-37 Rev 1

network

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

Source: NIST SP 800-53 Rev 4

network access

Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

Source: NIST SP 800-53 Rev 4

network defense

Programs, activities, and the use of tools necessary to facilitate them (including those governed by NSPD-54/HSPD-23 and NSD-42) conducted on a computer, network, or information or communications system by the owner or with the consent of the owner and, as appropriate, the users for the primary purpose of protecting (1) that computer, network, or system; (2) data stored on, processed on, or transiting that computer, network, or system; or (3) physical and virtual infrastructure controlled by that computer, network, or system. Network defense does not involve or require accessing or conducting activities on computers, networks, or information or communications systems without authorization from the owners or exceeding access authorized by the owners.

Source: PPD 20

network map

A representation of the internal network topologies and components down to the host/device level to include but not limited to: connection, sub-network, enclave, and host information.

network mapping

A process that discovers, collects, and displays the physical and logical information required to produce a network map.

Source: CNSSI No. 1012

network resilience

A computing infrastructure that provides continuous business operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands.

niche cross domain solution (CDS)

Cross domain solution that may (1) serve a specific narrow purpose, or (2) be built on very specialized hardware, or (3) be used in a special access program, and not appropriate for broader deployment.

no-lone zone (NLZ)
An area, room, or space that, when staffed, must be occupied by two or more appropriately cleared individuals who remain within sight of each other. See two-person integrity (TPI).

Source: CNSSI No. 4005 (COMSEC); NSA/CSS Manual Number 3-16 (COMSEC)

nonce
A random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing the transmittal of live data rather than replayed data, thus detecting and protecting against replay attacks.

Source: IETF RFC 4949 Ver 2

non-discretionary access control
See mandatory access control (MAC).

non-local maintenance
Maintenance activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network.

Source: NIST SP 800-53 Rev 4

non-organizational user
A user who is not an organizational user (including public users).

Source: NIST SP 800-53 Rev 4

non-person entity (NPE)
An entity with a digital identity that acts in cyberspace, but is not a human actor. This can include organizations, hardware devices, software applications, and information artifacts.

Source: DHS OIG 11-121

non-repudiation
Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

Source: NIST SP 800-53 Rev 4

NSA-approved commercial solution
The combination of multiple commercial-off-the-shelf (COTS) information assurance (IA) products in a layered configuration that satisfies the security requirements of an operational use case, when properly implemented in accordance with NSA-approved requirements and standards.

Source: CNSSAM IA-01-12

NSA-approved cryptography
Cryptography that consists of: (i) an approved algorithm; (ii) an implementation that has been approved for the protection of classified information in a particular environment; and (iii) a supporting key management infrastructure.

Source: NIST SP 800-53 Rev 4

NSA-approved product
Cryptographic equipment, assembly or component classified or certified by the National Security Agency (NSA) for encrypting and decrypting classified national security information and sensitive information when appropriately keyed. Developed using established NSA business processes and containing NSA approved algorithms.

NSS baselines

The combination of NIST SP 800-53 baselines (represented by an “X”) and the additional NIST SP 800-53 security controls required for National Security System (NSS) (represented by a “+”) that are applicable to NSS.

Source: CNSSI No. 1253

Nuclear Command and Control Information Assurance Material (NCCIM)

Information Assurance materials necessary to assure release of a nuclear weapon at the direction of the President and to secure against the unauthorized use of a nuclear weapon.

Source: NSA/CSS Policy 3-3

null

Dummy letter, letter symbol, or code group inserted into an encrypted message to delay or prevent its decryption or to complete encrypted groups for transmission or transmission security purposes.

object

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

Source: NIST SP 800-53 Rev 4

object reuse (C.F.D.)

Reassignment and reuse of a storage medium containing one or more objects after ensuring no residual data remains on the storage medium.

Rationale: Term has been replaced by the term “residual information protection”.

offensive cyberspace operations (OCO)

Cyberspace operations intended to project power by the application of force in or through cyberspace.

Source: DoD JP 3-12

official information

All information of any kind, however stored, that is in the custody and control of the Department/Agency (D/A), relates to information in the custody and control of the D/A, or was acquired by D/A employees, or former employees, as part of their official duties or because of their official status within the D/A while such individuals were employed by or served on behalf of the D/A.

Source: Title 6 CFR 5.41

off-line cryptosystem

Cryptographic system in which encryption and decryption are performed independently of the transmission and reception functions.

one-part code

Code in which plain text elements and their accompanying code groups are arranged in alphabetical, numerical, or other systematic order, so one listing serves for both encoding and decoding. One-part codes are normally small codes used to pass small volumes of low-sensitivity information.

one-time cryptosystem

Cryptosystem employing key used only once.

one-time pad (OTP)

Manual one-time cryptosystem produced in pad form.

one-time tape (OTT)

Punched paper tape used to provide key streams on a one-time basis in certain machine cryptosystems.

one-way hash algorithm

Hash algorithms which map arbitrarily long inputs into a fixed-size output such that it is very difficult (computationally infeasible) to find two different hash inputs that produce the same output. Such algorithms are an essential part of the process of producing fixed-size digital signatures that can both authenticate the signer and provide for data integrity checking (detection of input modification after signature).

Source: NIST SP 800-49

one-way transfer device

A hardware or software mechanism that only permits data to move in one direction and does not allow the flow of data in the opposite direction.

ongoing assessment and authorization

See information security continuous monitoring (ISCM).

ongoing authorization

See information security continuous monitoring (ISCM).

online cryptosystem

Cryptographic system in which encryption and decryption are performed in association with the transmitting and receiving functions.

open storage

1. Any storage of classified national security information outside of approved containers. This includes classified information that is resident on information systems media and outside of an approved storage container, regardless of whether or not that media is in use (i.e., unattended operations). Open storage of classified cryptographic material and equipment must be done within an approved COMSEC facility, vault, or secure room when authorized personnel are not present.

Source: CNSSI No. 4005 (COMSEC)

2. Storage of classified information within an approved facility not requiring use of General Services Administration-approved storage containers while the facility is not occupied by authorized personnel.

Source: ICS 700-1

open vulnerability assessment language (OVAL)

A language for representing system configuration information, assessing machine state, and reporting assessment results.

Source: NIST SP 800-126 Rev 2

operational controls (C.F.D.)

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).

Rationale: NIST SP 800-53 no longer includes the concept of operational, management, or technical controls, as it is not always clear which category any given control belongs.

operational key

Key intended for use over-the-air for protection of operational information or for the production or secure electrical transmission of key streams.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

operational resilience

The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions.

Source: DoDI 8500.01

operational waiver

Authority for continued use of unmodified COMSEC end-items pending the completion of a mandatory modification.

operations code (OPCODE)

Code composed largely of words and phrases suitable for general communications use.

operations security (OPSEC)

1. A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and determine which of these represent an unacceptable risk; then select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level.

Source: DoDD 5205.02E, DoD Operations Security (OPSEC) Program, June 20, 2012

2. A systematic and proven process intended to deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: (1) identification of critical information; (2) analysis of threats; (3) analysis of vulnerabilities; (4) assessment of risks; and (5) application of appropriate countermeasures.

Source: ICS 700-1

optional modification

National Security Agency (NSA)-approved modification not required for universal implementation by all holders of a COMSEC end-item. This class of modification requires all of the engineering/doctrinal control of mandatory modification but is usually not related to security, safety, TEMPEST, or reliability. See mandatory modification (MAN).

ordering privilege manager (OPM)

The key management entity (KME) authorized to designate other KME as a short title assignment requester (STAR) or ordering privilege manager (OPM).

Source: CNSSI No. 4005 (COMSEC)

organization

An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency, or, as appropriate, any of its operational elements). See enterprise.

Source: NIST SP 800-37 Rev 1

organizational registration authority (ORA)

Entity within the public key infrastructure (PKI) that authenticates the identity and the organizational affiliation of the users.

outside(r) threat

An unauthorized entity outside the security domain that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Source: NIST SP 800-32 (adapted)

overlay

A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.

Source: NIST SP 800-53 Rev 4

overt channel

Communications path within a computer system or network designed for the authorized transfer of data. See covert channel.

over-the-air key distribution (OTAD)

Providing electronic key via over-the-air rekeying, over-the-air key transfer, or cooperative key generation.

over-the-air key transfer (OTAT)

Electronically distributing key without changing traffic encryption key used on the secured communications path over which the transfer is accomplished.

over-the-air rekeying (OTAR)

Changing traffic encryption key or transmission security key in remote cryptographic equipment by sending new key directly to the remote cryptographic equipment over the communications path it secures.

overwrite

Writing one or more patterns of data on top of the physical location of data stored on the media.

Source: NIST SP 800-88 Rev 1

overwrite procedure (C.F.D.)

A software process that replaces data previously stored on storage media with a predetermined set of meaningless data or random patterns.

Rationale: Definition is obvious based on definition of overwrite.

packet sniffer

Software that observes and records network traffic.

page check

The verification of the presence of each required page in a physical publication.

Source: CNSSI No. 4005 (COMSEC)

parity (C.F.D.)

Bit(s) used to determine whether a block of data has been altered.

Rationale: Term has been replaced by the term "parity bit".

parity bit (C.F.D.)

A checksum that is computed on a block of bits by computing the binary sum of the individual bits in the block and then discarding all but the low-order bit of the sum. See checksum.

Source: IETF RFC 4949 Ver 2

passive attack

An attack that does not alter systems or data.

passive wiretapping

The monitoring or recording of data that attempts only to observe a communication flow and gain knowledge of the data it contains, but does not alter or otherwise affect that flow.

Source: IETF RFC 4949 Ver 2 (adapted)

password

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

Source: NSA/CSS Manual Number 3-16 (COMSEC)

patch

A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component.

Source: ISO/IEC 19770-2

patch management

The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

peer entity authentication

The process of verifying that a peer entity in an association is as claimed.

peer entity authentication service

A security service that verifies an identity claimed by or for a system entity in an association.

Source: IETF RFC 4949 Ver 2

penetration

See intrusion.

penetration testing

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

Source: NIST SP 800-53 Rev 4

per-call key

Unique traffic encryption key generated automatically by certain secure telecommunications systems to secure single voice or data transmissions. See cooperative key generation (CKG).

performance reference model (PRM)

Framework for performance measurement providing common output measurements throughout the Federal Government. It allows agencies to better manage the business of government at a strategic level by providing a means for using an agency's enterprise architecture (EA) to measure the success of information systems investments and their impact on strategic outcomes.

perimeter (C.F.D.)

1. Encompasses all those components of the system that are to be accredited by the DAA, and excludes separately accredited systems to which the system is connected.

2. Encompasses all those components of the system or network for which a body of evidence is provided in support of a formal approval to operate.

Rationale: Listed for deletion in 2010 version of CNSS 4009.

periods processing

1. A mode of system operation in which information of different sensitivities is processed at distinctly different times by the same system, with the system being properly purged or sanitized between periods.

Source: IETF RFC 4949 Ver 2

2. A method of sequential operation of an information system (IS) that provides the capability to process information at various levels of sensitivity at distinctly different times.

Source: DoD 5220.22-M

perishable data

Information whose value can decrease substantially during a specified time. A significant decrease in value occurs when the operational circumstances change to the extent that the information is no longer useful.

persona

1. An electronic identity that can be unambiguously associated with a single person or non-person entity (NPE). A single person or NPE may have multiple personas, with each persona being managed by the same or different organizations.

Source: ICTS UIAS v2

2. In military cyberspace operations, an abstraction of logical cyberspace with digital representations of individuals or entities in cyberspace, used to enable analysis and targeting. May be associated with a single or multiple entities.

Source: DoD JP 3-12

personal identification number (PIN)

A secret that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits.

Source: FIPS PUB 201-1

personal identity verification (PIV)

A physical artifact (e.g., identity card, “smart” card) issued to a government individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). PIV requirements are defined in FIPS PUB 201.

Source: CNSSI No. 1300

personal identity verification (PIV) authorization

The official management decision to authorize operation of a PIV Card Issuer after determining that the Issuer’s reliability has satisfactorily been established through appropriate assessment and certification processes.

personal identity verification (PIV) authorizing official

An individual who can act on behalf of an agency to authorize the issuance of a credential to an applicant.

personal identity verification (PIV) card

A physical artifact (e.g., identity card, “smart” card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so the claimed identity of the cardholder may be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

Source: FIPS PUB 201-1; CNSSI No. 1300

personally identifiable information(PII)

Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Source: NIST SP 800-122

personnel registration manager

The management role that is responsible for registering human users, i.e., users that are people.

phishing

A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.

Source: IETF RFC 4949 Ver 2

physically protected space (PPS)

A space inside one physically protected perimeter. Separate areas of equal protection may be considered part of the same PPS if the communication links between them are provided sufficient physical protection.

Source: CNSSI No. 5002

plain text

Unencrypted information that may be input to an encryption operation.

Source: IETF RFC 4949 Ver 2 (adapted)

Note: Plain text is not a synonym for clear text. See clear text.

plan of action and milestones(POA&M)

A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Source: OMB Memorandum 2-01; NIST SP 800-37 Rev 1

platform IT (PIT)

Information technology (IT), both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

Source: DoDI 8500.1

platform IT (PIT) system

A collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

Source: DoDI 8500.01

policy based access control (PBAC)

A form of access control that uses an authorization policy that is flexible in the types of evaluated parameters (e.g., identity, role, clearance, operational need, risk, heuristics).

policy decision point (PDP)

A system entity that makes authorization decisions for itself or for other system entities that request such decisions.

Source: NIST IR 7657

policy enforcement point (PEP)

A system entity that requests and subsequently enforces authorization decisions.

Source: NIST IR 7657

port scan

A technique that sends client requests to a range of service port addresses on a host.

Source: IETF RFC 4949 Ver 2

portable electronic device (PED)

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

Source: ICS 700-1

portable storage device

Portable device that can be connected to an information system (IS), computer, or network to provide data storage. These devices interface with the IS through processing chips and may load driver software, presenting a greater security risk to the IS than non-device media, such as optical discs or flash memory cards.

Note: Examples include, but are not limited to: USB flash drives, external hard drives, and external solid state disk (SSD) drives. Portable Storage Devices also include memory cards that have additional functions aside from standard data storage and encrypted data storage, such as built-in Wi-Fi connectivity and global positioning system (GPS) reception.

See also removable media.

positive control material

Generic term referring to a sealed authenticator system, permissive action link, coded switch system, positive enable system, or nuclear command and control documents, material, or devices.

potential impact

The loss of confidentiality, integrity, or availability that could be expected to have a limited (low) adverse effect, a serious (moderate) adverse effect, or a severe or catastrophic (high) adverse effect on organizational operations, organizational assets, or individuals.

Source: FIPS PUB 199 (adapted)

precursor

A sign that an attacker may be preparing to cause an incident.

Source: NIST SP 800-61 Rev 2

See indicator.

primary services node (PRSN)

A Key Management Infrastructure (KMI) core node that provides the users’ central point of access to KMI products, services, and information.

principal accrediting authority (PAA) (C.F.D.)

Senior official with authority and responsibility for all intelligence systems within an agency.

Rationale: PAA was used in both the IC and the DoD, but with the publication of ICD 503, the IC no longer uses the term PAA. Within the DoD, the transition to the RMF changed the term to principal authorizing official (PAO). See principal authorizing official (PAO).

principal authorizing official (PAO)

A senior (federal) official or executive with the authority to oversee and establish guidance for the strategic implementation of cybersecurity and risk management within their mission areas (i.e., the warfighting mission area (WMA), business mission area (BMA), enterprise information environment mission area (EIEMA), and DoD portion of the intelligence mission area (DIMA) as defined in DoDI 8115.02).

Source: DoDI 8500.01 (adapted)

privacy impact assessment (PIA)

An analysis of how information is handled 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Source: OMB Memorandum 3-22

private key

A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.

Source: CNSSI No. 1300

privilege

A right granted to an individual, a program, or a process.

privilege certificate manager (PCM)

The key management entity (KME) authorized to create the privilege certificate for another KME.

Source: CNSSI No. 4005 (COMSEC)

privileged account

An information system account with approved authorizations of a privileged user.

Source: NIST SP 800-53 Rev 4 (adapted)

privileged command

A human-initiated command executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information.

Source: NIST SP 800-53 Rev 4

privileged process

A computer process that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary processes are not authorized to perform.

privileged user

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

proactive cyber defense

A continuous process to manage and harden devices and networks according to known best practices.

Source: DSOC 2011

probability of occurrence

See likelihood of occurrence.

Source: NIST IR 7298 Rev 2

probe

A technique that attempts to access a system to learn something about the system.

process hijacking

A process checkpoint and migration technique that uses dynamic program re-writing techniques to add a checkpointing capability to a running program. Process hijacking makes it possible to checkpoint and migrate proprietary applications that cannot be re-linked with a checkpoint library allowing dynamic hand off of an ordinary running process to a distributed resource management system (e.g., the ability to trick or bypass the firewall allowing the server component to take over processes and gain rights for accessing the internet).

Source: CNSSI No. 1011

product compliant list (PCL)

The list of information assurance (IA) and IA-enabled products evaluated and validated pursuant to the NIAP program.

Source: CNSSP No. 11 (adapted)

product source node (PSN)

The Key Management Infrastructure core node that provides central generation of cryptographic key material.

profiling

Measuring the characteristics of expected activity so that changes to it can be more easily identified.

Source: NIST SP 800-61 Rev 2

proprietary information (PROPIN)

Material and information relating to or associated with a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know- how that has been clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the Government or to the public without restriction from another source.

proscribed information

<FOCI> Top Secret (TS) information, COMSEC information excluding controlled cryptographic items when unkeyed and utilized with unclassified keys, restricted data (RD), special access program (SAP) information, or sensitive compartmented information (SCI).

Source: DoDM 5220.22 Vol 3

protected distribution system (PDS)

Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.

Source: CNSSAM TEMPEST/01-13; NSA/CSS Policy 3-12

protection philosophy

Informal description of the overall design of an information system delineating each of the protection mechanisms employed. Combination of formal and informal techniques, appropriate to the evaluation class, used to show the mechanisms are adequate to enforce the security policy.

protection profile

A minimal, baseline set of requirements targeted at mitigating well defined and described threats. The term Protection Profile refers to NSA/NIAP requirements for a technology and does not imply or require the use of Common Criteria as the process for evaluating a product. Protection Profiles may be created by Technical Communities and will include:

- a set of technology-specific threats derived from operational knowledge and technical expertise;
- a set of core functional requirements necessary to mitigate those threats and establish a basic level of security for a particular technology; and,
- a collection of assurance activities tailored to the technology and functional requirements that are transparent, and produce achievable, repeatable, and testable results scoped such that they can be completed within a reasonable timeframe.

Source: CNSSP No. 11

protective packaging

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

Source: NSA/CSS Manual Number 3-16 (COMSEC)

protective technologies

Special tamper-evident features and materials employed for the purpose of detecting, tampering and deterring attempts to compromise, modify, penetrate, extract, or substitute information processing equipment and keying material.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

protocol

A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems.

Source: IETF RFC 4949 Ver 2

proxy

An application that “breaks” the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it.

Note: This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization’s internal network. Proxy servers are available for common Internet services; for example, a hyper text transfer protocol (HTTP) proxy used for Web access, and a simple mail transfer protocol (SMTP) proxy used for e-mail.

Source: NIST SP 800-44 Rev 2

proxy agent

A software application running on a firewall or on a dedicated proxy server that is capable of filtering a protocol and routing it between the interfaces of the device.

proxy server

A server that services the requests of its clients by forwarding those requests to other servers.

pseudonym

1. A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing.

2. An assigned identity that is used to protect an individual’s true identity.

pseudorandom number generator (PRNG)

A deterministic computational process that has one or more inputs called "seeds", and it outputs a sequence of values that appears to be random according to specified statistical tests. A cryptographic PRNG has the additional property that the output is unpredictable, given that the seed is not known.

Source: IETF RFC 4949 Ver 2 (adapted)

public domain software

Software not protected by copyright laws of any nation that may be freely used without permission of or payment to the creator, and that carries no warranties from or liabilities to the creator.

public key

A mathematical key that has public availability and that applications use to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can encrypt messages or files that the corresponding private key can decrypt.

Source: CNSSI No. 1300

public key certificate

See certificate.

public key cryptography (PKC)

Encryption system that uses a public-private key pair for encryption and/or digital signature.

public key enabling (PKE)

The incorporation of the use of certificates for security services such as authentication, confidentiality, data integrity, and non-repudiation.

public key infrastructure (PKI)

The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates.

Source: CNSSI No. 1300

public seed

A starting value for a pseudorandom number generator. The value produced by the random number generator may be made public. The public seed is often called a “salt”.

purge

A method of sanitization that applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.

Source: NIST SP 800-88 Rev 1

quadrant

Short name referring to technology that provides tamper-resistant protection to cryptographic equipment.

quality of service

The measurable end-to-end performance properties of a network service, which can be guaranteed in advance by a Service Level Agreement between a user and a service provider, so as to satisfy specific customer application requirements.

Note: These properties may include throughput (bandwidth), transit delay (latency), error rates, priority, security, packet loss, packet jitter, etc.

random number generator (RNG)

A process that is invoked to generate a random sequence of values (usually a sequence of bits) or an individual random value.

Source: IETF RFC 4949 Ver 2

randomizer

Analog or digital source of unpredictable, unbiased, and usually independent bits. Randomizers can be used for several different functions, including key generation or to provide a starting state for a key generator.

real time reaction

Immediate response to a penetration attempt that is detected and diagnosed in time to prevent access.

reciprocity

Mutual agreement among participating enterprises to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.

Source: NIST SP 800-37 Rev 1

records

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

Source: NIST SP 800-53 Rev 4

records management (C.F.D.)

The process for tagging information for records keeping requirements as mandated in the Federal Records Act and the National Archival and Records Requirements.

recovery procedures

Actions necessary to restore data files of an information system and computational capability after a system failure.

RED

Information or messages that contain sensitive or classified information that is not encrypted. See also BLACK.

Source: CNSSI No. 4005 (COMSEC)

RED/BLACK concept

Separation of electrical and electronic circuits, components, equipment, and systems that handle national security information (RED), in electrical form, from those that handle non-national security information (BLACK) in the same form.

Source: CNSSAM TEMPEST/01-13; NTISSI 7002(TEMPEST)

RED data

Date that is not protected by encryption. Also known as unencrypted data.

Source: CNSSI No. 4005 (COMSEC)

RED equipment

A term applied to equipment that processes unencrypted national security information that requires protection during electrical/electronic processing.

Source: CNSSAM TEMPEST/01-13

RED key

Key that has not been encrypted in a system approved by NSA for key encryption or encrypted key in the presence of its associated key encryption key (KEK) or transfer key encryption key (TrKEK). Encrypted key in the same fill device as its associated KEK or TrKEK is considered unencrypted. (RED key is also known as unencrypted key). Such key is classified at the level of the data it is designed to protect. See BLACK data and encrypted key.

Source: CNSSI No. 4005 (COMSEC)

RED line

An optical fiber or a metallic wire that carries a RED signal or that originates/terminates in a RED equipment or system.

Source: CNSSAM TEMPEST/01-13

RED optical fiber line

An optical fiber that carries RED signal or that originates/terminates in RED equipment or system.

Source: CNSSAM TEMPEST/01-13

RED signal

Any electronic emission (e.g., plain text, key, key stream, subkey stream, initial fill, or control signal) that would divulge national security information if recovered.

Source: CNSSAM TEMPEST/01-13

Red Team

A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team.

RED wireline

A metallic wire that carries a RED signal or that originates/terminates in a RED equipment or system.

Source: CNSSAM TEMPEST/01-13

regenerative cyber defense

The process for restoring capabilities after a successful, large scale cyberspace attack, ideally in a way that prevents future attacks of the same nature.

Source: DSOC 2011

registration

The process through which a party applies to become a subscriber of a credentials service provider (CSP) and a registration authority validates the identity of that party on behalf of the CSP.

Source: NIST SP 800-63-2 (adapted)

registration authority (RA)

1. An entity authorized by the certification authority system (CAS) to collect, verify, and submit information provided by potential Subscribers which is to be entered into public key certificates. The term RA refers to hardware, software, and individuals that collectively perform this function.

Source: CNSSI No. 1300

2. The key management entity (KME) within each Service or Agency responsible for registering KMEs and assigning electronic key management system (EKMS) IDs to them.

Source: CNSSI No. 4005 (COMSEC)

regrader

A trusted process explicitly authorized to re-classify and re-label data in accordance with a defined policy exception. Untrusted /Unauthorized processes are such actions by the security policy.

Source: CNSSI No. 1253F Attachment 3

re-key (a certificate)

The process of creating a new certificate with a new validity period, serial number, and public key while retaining all other Subscriber information in the original certificate.

Source: CNSSI No. 1300

release prefix

Prefix appended to the short title of U.S.-produced keying material to indicate its foreign releasability. "A" designates material that is releasable to specific allied nations and "U.S." designates material intended exclusively for U.S. use.

relying party

An entity that relies on the validity of the binding of the Subscriber's name to a public key to verify or establish the identity and status of an individual, role, or system or device; the integrity of a digitally signed message; the identity of the creator of a message; or confidential communications with the Subscriber.

Source: CNSSI No. 1300

remanence

Residual information remaining on storage media after clearing. See magnetic remanence and clearing.

Source: IETF RFC 4949 Ver 2

remediation

The act of mitigating a vulnerability or a threat.

Source: NIST SP 800-40 Rev 2 (adapted)

remote access

Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

Source: NIST SP 800-53 Rev 4

remote diagnostics/ maintenance

Maintenance activities conducted by authorized individuals communicating through an external network (e.g., the Internet).

remote rekeying

Procedure by which a distant crypto-equipment is rekeyed electrically. See automatic remote rekeying and manual remote rekeying.

removable media

Portable data storage medium that can be added to or removed from a computing device or network.

Note: Examples include, but are not limited to: optical discs (CD, DVD, Blu-ray); external / removable hard drives; external / removable Solid State Disk (SSD) drives; magnetic / optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external / removable disks (floppy, Zip, Jaz, Bernoulli, UMD).

See also portable storage device.

removable media device

See portable storage device.

replay attacks

An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.

reserve keying material

Key held to satisfy unplanned needs. See contingency key.

resident alien

A citizen of a foreign nation, legally residing in the United States on a permanent basis, who is not yet a naturalized citizen of the United States.

Source: CNSSI No. 4005 (COMSEC)

residual information protection

Ensur(ing) that any data contained in a resource is not available when the resource is de-allocated from one object and reallocated to a different object.

Source: ISO/IEC 15408-2 (adapted)

residual risk

Portion of risk remaining after security measures have been applied.

Source: NIST SP 800-33 (adapted)

residue

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

resilience

The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Source: PPD 21

responsibility to provide

An information distribution approach whereby relevant essential information is made readily available and discoverable to the broadest possible pool of potential users.

restoration

The process of changing the status of a suspended (i.e., temporarily invalid) certificate to valid.

Source: CNSSI No. 1300

revocation

The process of permanently ending the binding between a certificate and the identity asserted in the certificate from a specified time forward.

Source: CNSSI No. 1300

risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.

Source: FIPS PUB 200 (adapted); NIST SP 800-37 Rev 1

risk adaptable access control (RAdAC)

A form of access control that uses an authorization policy that takes into account operational need, risk, and heuristics.

risk assessment

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

Source: NIST SP 800-39

risk assessment report (RAR).

The report which contains the results of performing a risk assessment or the formal output from the process of assessing risk.

Source: NIST SP 800-30 Rev 1

risk assessor

The individual, group, or organization responsible for conducting a risk assessment.

Source: NIST SP 800-30 Rev 1

risk executive (function)

An individual or group within an organization that helps to ensure that (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.

Source: NIST SP 800-37 Rev 1 (adapted)

risk management

The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

Source: NIST SP 800-39

risk management framework (RMF)

A structured approach used to oversee and manage risk for an enterprise.

risk mitigation

Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

risk response

Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.

Source: NIST SP 800-39

risk tolerance

The level of risk an entity is willing to assume in order to achieve a potential desired result.

Source: NIST SP 800-32

robustness

The ability of an information assurance (IA) entity to operate correctly and reliably across a wide range of operational conditions, and to fail gracefully outside of that operational range.

role

A job function or employment position to which people or other system entities may be assigned in a system.

Source: IETF RFC 4949 Ver 2

role-based access control (RBAC)

Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Source: NIST SP 800-53 Rev 4

root certificate authority

In a hierarchical public key infrastructure (PKI), the certification authority (CA) whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

Source: NIST SP 800-32

root user

See privileged user.

rootkit

A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.

rule-based security policy

A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access.

Source: NIST SP 800-33

Also known as discretionary access control (DAC).

ruleset

A table of instructions used by a controlled interface to determine what data is allowable and how the data is handled between interconnected systems.

safeguards

The protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Source: FIPS PUB 200

salt

A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker.

Source: NIST SP 800-63-2

sandboxing

A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized.

sanitization

See sanitize.

sanitize

1. A process to render access to target data on the media infeasible for a given level of effort. Clear, purge, damage, and destruct are actions that can be taken to sanitize media. See media sanitization.

Source: NIST SP 800-88 Rev 1

2. The removal of extraneous or potentially harmful data (e.g., malware) within a file or other information container (e.g., network protocol packet).

Source: CNSSI No. 1253F Attachment 3

scanning

Sending packets or requests to another system to gain information to be used in a subsequent attack.

scavenging

Searching through object residue to acquire data.

scoping considerations

A part of tailoring guidance providing organizations with specific considerations on the applicability and implementation of security controls in the security control baseline. Areas of consideration include policy/regulatory, technology, physical infrastructure, system component allocation, operational/environmental, public access, scalability, common control, and security objective.

Source: NIST SP 800-53 Rev 4

secret key

A cryptographic key that is used with a (symmetric) cryptographic algorithm that is uniquely associated with one or more entities and is not made public. The use of the term “secret” in this context does not imply a classification level, but rather implies the need to protect the key from disclosure.

Source: NIST 800-57 Part 1 Rev 3

secret key (symmetric) cryptographic algorithm

A cryptographic algorithm that uses a single key (i.e., a secret key) for both encryption and decryption.

Source: FIPS PUB 140-2 (adapted)

secret seed

A secret value used to initialize a pseudorandom number generator.

secure communication protocol

A communication protocol that provides the appropriate confidentiality, authentication, and content-integrity protection.

Source: NIST SP 800-57 Part 1 Rev 3

secure communications

Telecommunications deriving security through use of National Security Agency (NSA)-approved products and/or protected distribution systems (PDSs).

secure communications interoperability protocol (SCIP) product

National Security Agency (NSA) certified secure voice and data encryption devices that provide interoperability with both national and foreign wired and wireless products.

Source: CNSSI No. 4032

secure hash algorithm (SHA)

A hash algorithm with the property that it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest.

Source: FIPS PUB 180-4 (adapted)

secure hash standard

The standard specifying hash algorithms that can be used to generate digests of messages. The digests are used to detect whether messages have been changed since the digests were generated.

Source: FIPS PUB 180-4

secure socket layer (SSL)

A protocol used for protecting private information during transmission via the Internet.

Note: SSL works by using the service public key to encrypt a secret key that is used to encrypt the data that is transferred over the SSL session. Most web browsers support SSL and many web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https:” instead of “http:”. The default port for SSL is 443.

secure state

Condition in which no subject can access any object in an unauthorized manner.

secure/ multipurpose internet mail extensions (S/MIME)

A set of specifications for securing electronic mail. S/MIME is based upon the widely used MIME standard and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The basic security services offered by S/MIME are authentication, non-repudiation of origin, message integrity, and message privacy. Optional security services include signed receipts, security labels, secure mailing lists, and an extended method of identifying the signer’s certificate(s).

Source: NIST SP 800-49

security

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

security assertion markup language (SAML)

A protocol consisting of XML-based request and response message formats for exchanging security information, expressed in the form of assertions about subjects, between on-line business partners.

security assessment report (SAR)

Provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls.

Source: DoDI 8510.01

security association

A relationship established between two or more entities to enable them to protect data they exchange.

security attribute

An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system which are used to enable the implementation of access control and flow control policies; reflect special dissemination, handling, or distribution instructions; or support other aspects of the information security policy.

Source: NIST SP 800-53 Rev 4

security auditor

A trusted role that is responsible for auditing the security of certification authority systems (CASs) and registration authorities (RAs), including reviewing, maintaining, and archiving audit logs and performing or overseeing internal audits of CASs and RAs.

Source: CNSSI No. 1300

security authorization (to operate)

See authorization to operate (ATO).

Source: NIST SP 800-37 Rev 1

security authorization package

Documents the results of the security control assessment and provides the authorizing official with essential information needed to make a risk-based decision on whether to authorize operation of an information system or a designated set of common controls.

Contains: (i) the security plan; (ii) the security assessment report (SAR); and (iii) the plan of action and milestones (POA&M).

Note: Many departments and agencies may choose to include the risk assessment report (RAR) as part of the security authorization package. Also, many organizations use system security plan in place of the security plan.

Source: NIST SP 800-37 Rev 1

security banner

1. A persistent visible window on a computer monitor that displays the highest level of data accessible during the current session.

2. The opening screen that informs users of the implications of accessing a computer resource (e.g. consent to monitor).

security category

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation.

Source:; FIPS PUB 199 (adapted)

security categorization

The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS PUB 199 for other than national security systems. See security category.

Source: NIST SP 800-53 Rev 4

security concept of operations (Security CONOP)

A security-focused description of an information system, its operational policies, classes of users, interactions between the system and its users, and the system's contribution to the operational mission.

security content automation protocol (SCAP)

A suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated, both to machines and humans.

Source: NIST SP 800-126 Rev 2

Note: There are six individual specifications incorporated into SCAP: CVE (common vulnerabilities and exposures); CCE (common configuration enumeration); CPE (common platform enumeration); CVSS (common vulnerability scoring system); OVAL (open vulnerability assessment language); and XCCDF (eXtensible configuration checklist description format).

security control assessment

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

Source: NIST SP 800-37 Rev 1

security control assessor (SCA)

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

Source: NIST SP 800-37 Rev 1

security control baseline

The set of minimum security controls defined for a low-impact, moderate- impact, or high-impact information system.

Source: FIPS PUB 200

security control enhancements

Statements of security capability to 1) build in additional, but related, functionality to a basic control; and/or 2) increase the strength of a basic control.

Source: NIST SP 800-53A Rev 1

security control inheritance

A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, and assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See common control.

Source: NIST SP 800-53A Rev 1

security control provider

An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems).

See common control provider.

Source: NIST SP 800-37 Rev 1 (adapted)

security controls

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Source: FIPS PUB 199

security domain

A domain that implements a security policy and is administered by a single authority.

Source: CNSSP No. 24; CNSSI No. 1253F Attachment 3

security engineering

An interdisciplinary approach and means to enable the realization of secure systems. It focuses on defining customer needs, security protection requirements, and required functionality early in the systems development lifecycle, documenting requirements, and then proceeding with design, synthesis, and system validation while considering the complete problem.

security fault analysis (SFA)

An assessment usually performed on information system hardware, to determine the security properties of a device when hardware fault is encountered.

security features users guide (SFUG) (C.F.D.)

Guide or manual explaining how the security mechanisms in a specific system work.

security filter

A secure subsystem of an information system that enforces security policy on the data passing through it.

security impact analysis

The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

Source: NIST SP 800-37 Rev 1

security incident

See incident.

Source: NIST IR 7298 Rev 2

security inspection

Examination of an information system to determine compliance with security policy, procedures, and practices.

security kernel
Hardware, firmware, and software elements of a trusted computing base implementing the reference monitor concept. Security kernel must mediate all accesses, be protected from modification, and be verifiable as correct.

security label
The means used to associate a set of security attributes with a specific information object as part of the data structure for that object.

Source: NIST SP 800-53 Rev 4

security marking
The means used to associate a set of security attributes with objects in a human-readable form, to enable organizational process-based enforcement of information security policies.

Source: NIST SP 800-53 Rev 4

security mechanism
A device or function designed to provide one or more security services usually rated in terms of strength of service and assurance of the design.

security perimeter
A physical or logical boundary that is defined for a system, domain, or enclave; within which a particular security policy or security architecture is applied.

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

See system security plan or information security program plan.

Source: NIST SP 800-53; SP 800-53A; SP 800-37 Rev 1; NIST SP 800-18 Rev 1

security policy
A set of criteria for the provision of security services.

Source: NIST SP 800-53 Rev 4

security posture
The security status of an enterprise's networks, information, and systems based on information assurance (IA) resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

security program plan
Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management security controls and common security controls in place or planned for meeting those requirements.

security protocol
An abstract or concrete protocol that performs security-related functions.

Source: CNSSP No. 15

security range
Highest and lowest security levels that are permitted in or on an information system, system component, subsystem, or network.

See system high and system low.

security-relevant change
Any change to a system's configuration, environment, information content, functionality, or users which has the potential to change the risk imposed upon its continued operations.

security-relevant event

An occurrence (e.g., an auditable event or flag) considered to have potential security implications to the system or its environment that may require further action (noting, investigating, or reacting).

security requirements

Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Source: FIPS PUB 200

security requirements baseline

Description of the minimum requirements necessary for an information system to maintain an acceptable level of risk.

security requirements guide (SRG)

Compilation of control correlation identifiers (CCIs) grouped in more applicable, specific technology areas at various levels of technology and product specificity. Contains all requirements that have been flagged as applicable from the parent level regardless if they are selected on a Department of Defense (DoD) baseline or not.

Source: DoDI 8500.01

security requirements traceability matrix (SRTM)

Matrix documenting the system's agreed upon security requirements derived from all sources, the security features' implementation details and schedule, and the resources required for assessment.

security safeguards

Protective measures and controls prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

security service

A capability that supports one, or many, of the security goals. Examples of security services are key management, access control, and authentication.

Source: NIST SP 800-27 Rev A

security strength

A number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system. In this policy, security strength is specified in bits and is a specific value from the set {80, 112, 128, 192, 256}.

Source: CNSSI No. 1300

security target

An implementation-dependent statement of security needs for a specific identified target of evaluation (TOE).

Source: ISO/IEC 15408-1

security technical implementation guide (STIG)

Based on Department of Defense (DoD) policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DoD baseline.

Source: DoDI 8500.01

security test and evaluation (ST&E)

Examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of that system.

seed key

Initial key used to start an updating or key generation process.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

self-encrypting devices / self-encrypting drives (SED)

Data storage device with built-in cryptographic processing that may be utilized to encrypt and decrypt the stored data, occurring within the device and without dependence on a connected information system.

Source: NIST SP 800-88 Rev 1 (adapted)

senior agency information security officer (SAISO)

Official responsible for carrying out the chief information officer (CIO) responsibilities under the Federal Information Security Management Act (FISMA) and serving as the CIO's primary liaison to the agency's authorizing officials, information system owners, and information systems security officers.

Note: Also known as senior information security officer (SISO) or chief information security officer (CISO).

Source: FIPS PUB 200 (adapted from 44 U.S.C. Sec. 3544)

senior information security officer (SISO)

See senior agency information security officer (SAISO).

Source: NIST SP 800-37 Rev 1

sensitive compartmented information (SCI)

1. A subset of Classified National Intelligence concerning or derived from intelligence sources, methods, or analytical processes, that is required to be protected within formal access control systems established by the Director of National Intelligence.

Source: ICD 703

2. Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

Sensitive Compartmented Information Facility (SCIF)

An area, room, group of rooms, buildings, or installation certified and accredited as meeting Director of National Intelligence security standards for the processing, storage, and/or discussion of sensitive compartmented information (SCI).

Source: ICS 700-1

sensitive information

See controlled unclassified information (CUI).

Note: The term sensitive information as well as others such as For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) will no longer be used upon implementation of 32 CFR 2002.

sensitivity

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

Source: NIST SP 800-60 Vol 1 Rev 1

service authority (COMSEC)

The COMSEC Service Authority is the Department/Agency (D/A) senior staff component/command level element that provides staff supervision and oversight of COMSEC operations, policies, procedures, accounting, resource management, material acquisition, and training throughout the D/A. The multitude of responsibilities inherent to the COMSEC Service Authority functions may be allocated to one or more senior staff elements, while specific oversight and execution of selected functional responsibilities may be delegated to subordinate field agencies and activities.

Source: CNSSI No. 4005 (COMSEC)

service level agreement (SLA)

Defines the specific responsibilities of the service provider and sets the customer expectations.

shielded enclosure

Room or container designed to attenuate electromagnetic radiation, acoustic signals, or emanations.

short title

Identifying combination of letters and numbers assigned to certain COMSEC materials to facilitate handling, accounting, and controlling (e.g., KAM-211, KG-175). Each item of accountable COMSEC material is assigned a short title to facilitate handling, accounting and control.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

short title assignment requester (STAR)

The key management entity (KME) privileged to request assignment of a new short title and generation of key against that short title.

Source: CNSSI No. 4005 (COMSEC)

signaling rate

The signaling rate of a digital signal is defined as the reciprocal of the bit width (1/bit width). The signaling rate is used to determine the frequency range of electrical isolation.

Source: CNSSAM TEMPEST/01-13

signature

A recognizable, distinguishing pattern. See attack signature and digital signature.

Source: NIST SP 800-61 Rev 2 (adapted)

signature certificate

A public key certificate that contains a public key intended for verifying digital signatures rather than authenticating, encrypting data or performing any other cryptographic functions.

Source: CNSSI No. 1300; NIST SP 800-32

significant consequences

Loss of life, significant responsive actions against the United States, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States.

Source: PPD 20

single point keying (SPK)

Means of distributing key to multiple, local crypto equipment or devices from a single fill point.

situational awareness

Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future.

smart card

A credit card-sized card with embedded integrated circuits that can store, process, and communicate information.

smart data

Association of authority, access requirements, retention provenance and any additional information with a data object; smart data includes data provenance and data tagging.

Source: NSA/CSS IAD Guidance No. 400

sniffer

See packet sniffer and passive wiretapping.

social engineering

An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

Source: NIST SP 800-61 Rev 2

software

Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution.

Source: IETF RFC 4949 Ver 2

software assurance (SwA)

1. The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.

Source: DoDI 5200.44

2. The planned and systematic set of activities that ensure that software life cycle processes and products conform to requirements, standards, and procedures.

Source: NASA-STD 8739.8

software identification (SWID) tag

A set of structured data elements containing authoritative identification information about a software component.

Source: ISO/IEC 19770-2

software system test and evaluation process

Process that plans, develops, and documents the qualitative/quantitative demonstration of the fulfillment of all baseline functional performance, operational, and interface requirements.

spam

Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

spear phishing

A colloquial term that can be used to describe any highly targeted phishing attack.

Source: DoJ Report on Phishing

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.

Source: ICS 700-1

special access program facility (SAPF)

A specific physical space that has been formally accredited in writing by the cognizant program security officer (PSO) that satisfies the criteria for generating, safeguarding, handling, discussing, and storing classified or unclassified program information, hardware, and materials.

Source: DoDM 5205.07

special category

Sensitive compartmented information (SCI), special access program (SAP) information, or other compartment information.

Source: CNSSAM TEMPEST/01-13

special character

Any non-alphanumeric character that can be rendered on a standard, American-English keyboard. Use of a specific special character may be application dependent. The list of 7-bit ASCII special characters follows: ` ~! @ # $ % ^ & * ( ) _ + | } { “ : ? > < [ ] \ ; ’ , . / - =

spillage

Security incident that results in the transfer of classified information onto an information system not authorized to store or process that information.

split knowledge

1. Separation of data or information into two or more parts, each part constantly kept under control of separate authorized individuals or teams so that no one individual or team will know the whole data.

2. A process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, which can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key.

Source: NIST SP 800-57 Part 1 Rev 3 (adapted)

spoofing

1. Faking the sending address of a transmission to gain illegal entry into a secure system.

2. The deliberate inducement of a user or resource to take incorrect action.

Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.

spread spectrum

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

spyware

Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

Source: NIST SP 800-53 Rev 4

steganography

The art, science, and practice of communicating in a way that hides the existence of the communication.

Source: NIST SP 800-72 (adapted)

strength of mechanism (SoM)

A scale for measuring the relative strength of a security mechanism.

striped core

A network architecture in which user data traversing a core IP network is decrypted, filtered and re-encrypted one or more times.

Note: The decryption, filtering, and re-encryption are performed within a “Red gateway”; consequently, the core is “striped” because the data path is alternately Black, Red, and Black.

strong authentication

A method used to secure computer systems and/or networks by verifying a user’s identity by requiring two-factors in order to authenticate (something you know, something you are, or something you have).

Source: DoDI 8420.01

subaccount

A COMSEC account that only received key from, and only reports to, its parent account, never a Central Office of Record.

Source: CNSSI No. 4005 (COMSEC)

subassembly

Two or more parts that form a portion of an assembly or a unit replaceable as a whole, but having a part or parts that are individually replaceable.

Source: CNSSI No. 4033

sub-hand receipt

The hand receipt of COMSEC material to authorized individuals by persons to whom the material has already been hand receipted.

Source: CNSSI No. 4005 (COMSEC)

subject

Generally an individual, process, or device causing information to flow among objects or change to the system state. See object.

Source: NIST SP 800-53 Rev 4

subordinate certificate authority

In a hierarchical public key infrastructure (PKI), a certificate authority (CA) whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. See superior certification authority.

Source: CNSSI No. 1300

subscriber

An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate.

Source: CNSSI No. 1300

Suite A

A specific set of classified cryptographic algorithms used for the protection of some categories of restricted mission critical information.

Suite B

A specific set of cryptographic algorithms suitable for protecting both classified and unclassified national security systems, classified national security information, and sensitive information throughout the U.S. government and to support interoperability with allies and coalition partners.

Suite B compatible

An information assurance (IA) or IA-enabled information technology (IT) product that:
a. Uses National Security Agency (NSA)-approved public standards-based security protocols. If none are available with the necessary functionality, then uses a NSA-approved security protocol;
b. Includes (as selectable capabilities) all of the Suite B cryptographic algorithms that are functionally supported by the NSA-approved security protocol(s); and
c. Has been evaluated or validated in accordance with NSTISSP 11.

Source: CNSSP No. 15

superencryption

1. The encrypting of already encrypted information.

2. An encryption operation for which the plaintext input to be transformed is the ciphertext output of a previous encryption operation.

Source: IETF RFC 4949 Ver 2

superior certification authority

In a hierarchical public key infrastructure (PKI), a certification authority (CA) who has certified the certificate signature key of another CA, and who constrains the activities of that CA. See subordinate certification authority.

Source: NIST SP 800-32

supersession

The scheduled or unscheduled replacement of COMSEC material with a different edition.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

superuser

See privileged user.

supervisory control and data acquisition (SCADA)

A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated.

Source: NIST SP 800-82 Rev 1

supply chain

A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.

supply chain assurance

Confidence that the supply chain will produce and deliver elements, processes, and information that function as expected.

Source: NIST IR 7622

supply chain attack

Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.

supply chain risk

The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of a system (Ref: The Ike Skelton National Defense Authorization Act for Fiscal Year 2011).

Source: CNSSD No. 505

supply chain risk management (SCRM)

A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplies product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

Source: CNSSD No. 505

suppression measure

Action, procedure, modification, or device that reduces the level of, or inhibits the generation of, compromising emanations in an information system.

suspension

The process of changing the status of a valid certificate to suspended (i.e., temporarily invalid).

Source: CNSSI No. 1300

syllabary (C.F.D.)

List of individual letters, combination of letters, or syllables, with their equivalent code groups, used for spelling out words or proper names not present in the vocabulary of a code. A syllabary may also be a spelling table.

symmetric encryption algorithm

Encryption algorithms using the same secret key for encryption and decryption.

Source: NIST SP 800-49

symmetric key

A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.

Source: NIST SP 800-63-2

synchronous crypto-operation

Method of on-line cryptographic operation in which cryptographic equipment and associated terminals have timing systems to keep them in step.

system

Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. See information system (IS).

system administrator (SA)

Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures.

system development life cycle (SDLC)

The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

Source: NIST SP 800-34 Rev 1

system high

Highest security level supported by an information system.

system high mode (C.F.D.)

Information systems security mode of operation wherein each user, with direct or indirect access to the information system, its peripherals, remote terminals, or remote hosts, has all of the following: 1) valid security clearance for all information within an information system; 2) formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, sub compartments and/or special access programs); and 3) valid need-to- know for some of the information contained within the information system.

Rationale: system high, along with other related terms, has been listed for deletion.

system indicator

Symbol or group of symbols in an off-line encrypted message identifying the specific cryptosystem or key used in the encryption.

system integrity

The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

Source: NIST SP 800-27 Rev A

system interconnection

The direct connection of two or more information systems for the purpose of sharing data and other information resources.

Source: NIST SP 800-47

system low

Lowest security level supported by an information system.

system or device certificate

The system or device whose name appears as the subject in a certificate.

Source: CNSSI No. 1300

system owner

Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.

systems security engineering

Systems security engineering is a specialty engineering field strongly related to systems engineering. It applies scientific, engineering, and information assurance principles to deliver trustworthy systems that satisfy stakeholder requirements within their established risk tolerance.

See also information systems security engineering (ISSE).

Source: NIST SP 800-160(draft)

systems security officer (SSO)

See information systems security officer (ISSO).

Source: NIST IR 7298 Rev 2

system security plan (SSP)

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

Source: NIST SP 800-18 Rev 1

system-specific security control

A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.

Source: NIST SP 800-53 Rev 4

tactical data

Information that requires protection from disclosure and modification for a limited duration as determined by the originator or information owner.

tactical edge

The platforms, sites, and personnel (U. S. military, allied, coalition partners, first responders) operating at lethal risk in a battle space or crisis environment characterized by 1) a dependence on information systems and connectivity for survival and mission success, 2) high threats to the operational readiness of both information systems and connectivity, and 3) users are fully engaged, highly stressed, and dependent on the availability, integrity, and transparency of their information systems.

tailoring

The process by which a security control baseline is modified based on (i) the application of scoping guidance, (ii) the specification of compensating security controls, if needed, and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.

Source: NIST SP 800-37 Rev 1

tampering

An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data.

Source: DHS, Information Technology Sector Baseline Risk Assessment (adapted)

target of evaluation (TOE)

In accordance with Common Criteria, an information system, part of a system or product, and all associated documentation, that is the subject of a security evaluation.

technical community (TC)

Government/Industry/Academia partnerships formed around major technology areas to act like a standards body for the purpose of creating and maintaining Protection Profiles.

Source: CNSSP No. 11

technical reference model (TRM)

A component-driven, technical framework that categorizes the standards and technologies to support and enable the delivery of service components and capabilities.

technical security controls

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

technical security material

Equipment, components, devices, and associated documentation or other media which pertain to cryptography, or to the security of telecommunications and information systems.

Source: CNSSP No. 8

technical surveillance countermeasures (TSCM)

Techniques to detect, neutralize, and exploit technical surveillance technologies and hazards that permit the unauthorized access to or removal of information.

Source: DoDI 5240.05

technical vulnerability information

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

telecommunications

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

Source: NSA/CSS Manual Number 3-16 (COMSEC); NSTISSD 501

telecommunications security (TSEC) nomenclature

The National Security Agency (NSA) system for identifying the type and purpose of certain items of COMSEC material.

Source: CNSSI No. 4005 (COMSEC)

TEMPEST

A name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment.

Source: FIPS PUB 140-2

TEMPEST certified equipment or system

Equipment or systems that have been certified to meet the applicable level of NSTISSAM TEMPEST/1-92 or previous editions. Typically categorized as Level 1 for the highest containment of classified signals; Level II for the moderate containment of classified signals; and Level III for the least containment of classified signals.

Source: CNSSAM TEMPEST/01-13

TEMPEST zone

Designated area within a facility where equipment with appropriate TEMPEST characteristics (TEMPEST zone assignment) may be operated.

test key

Key intended for testing of COMSEC equipment or systems. If intended for off-the-air, in-shop use, such key is called maintenance key.

Source: CNSSI No. 4005 (COMSEC)

threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Source: NIST SP 800-30 Rev 1

threat analysis

See threat assessment.

threat assessment

Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

threat monitoring

Analysis, assessment, and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security.

threat source

The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.

Source: FIPS PUB 200

Tier 0 (central facility) (COMSEC)

The composite facility approved, managed, and operated under National Security Agency (NSA) oversight that includes:

a. National COMSEC Material Generation and Production facilities for physical and electronic keys, both traditional and modern.

b. Central Office of Record (COR) services for NSA, contractor, and select Civil Agency accounts.

c. National Distribution Authority (NDA) for U.S. accounts worldwide.

d. National Registration Authority for all non-military accounts on U.S. systems.

e. National Credential Manager for all electronic key management system (EKMS) accounts on U.S. systems.

f. EKMS Defense Courier Service (DCS) data administrator.

Source: CNSSI No. 4005 (COMSEC)

Tier 1/common tier 1 (CTI) (COMSEC)

The composite of the electronic key management system (EKMS) Common Tier 1 (CT1) systems that is a tool used by the military service central offices of record (CORs) to support their accounts and by the Civil Agency CORs requesting CT1 support. The CT1 also provides generation and distribution of many types of traditional keying material for large nets. The CT1 consists of two Primary Tier 1 sites, one Extension Tier 1 site, and other Physical Material Handling Segments (PMHS) at several service sites providing the following services:

a. Common military traditional electronic keying material generation and distribution facilities.

b. Common keying material ordering interface for all types of keying material required by military accounts.

c. Registration Authority for U.S. military accounts.

d. Ordering Privilege Manager for U.S. military accounts.

e. Management for the military's COMSEC vaults, depots, and logistics system facilities.

Note: The responsibilities of the CT1 include COMSEC material accounting, inventories, keying material distribution, and privilege management. Those COMSEC activity functions that cannot be performed by the CT1 have been consolidated under the role of the Service Authority.

Source: CNSSI No. 4005 (COMSEC)

Tier 2 (COMSEC)

The layer of the electronic key management system (EKMS) comprising COMSEC accounts and subaccounts managing keying material and other COMSEC material. Automated EKMS Tier 2s consist of a Service- or Agency-provided Local Management Device (LMD) running the Local COMSEC Management Software (LCMS), a Key Processor (KP), and a secure terminal equipment (STE) or other secure communication device(s).

Note: Some Tier 2 accounts or subaccounts operate an local management device (LMD) without a KP.

Source: CNSSI No. 4005 (COMSEC)

Tier 3 (COMSEC)

The lowest tier or layer of electronic key management system (EKMS) architecture comprising hand-receipt holders who use an electronic fill device (e.g., the Data Transfer Device (DTD), Secure DTD2000 System (SDS), Simple Key Loader (SKL)) and all other means to issue key to End Cryptographic Units (ECUs). Tier 3 elements receive keying material from Tier 2 activities by means of electronic fill devices or in canisters (for physical keying material).

Source: CNSSI No. 4005 (COMSEC)

time bomb

Resident computer program that triggers an unauthorized act at a predefined time.

time-compliance date

Date by which a mandatory modification to a COMSEC end-item must be incorporated if the item is to remain approved for operational use.

time-dependent password

Password that is valid only at a certain time of day or during a specified interval of time.

token

Something that the claimant possesses and controls (such as a key or password) that is used to authenticate a claim. See cryptographic token.

Source: NIST SP 800-63-2 (adapted)

tradecraft identity

An identity used for the purpose of work-related interactions that may or may not be synonymous with an individual's true identity.

traditional key

Term used to reference symmetric key wherein both ends of a link or all parties in a cryptonet have the same exact key. 256-bit advanced encryption standard (AES), high assurance internet protocol encryptor (HAIPE) pre-placed, and authenticated pre-placed key are examples of traditional key.

Source: CNSSI No. 4006

traffic analysis (TA)

Gaining knowledge of information by inference from observable characteristics of a data flow, even if the information is not directly available (e.g., when the data is encrypted). These characteristics include the identities and locations of the source(s) and destination(s) of the flow, and the flow's presence, amount, frequency, and duration of occurrence.

traffic encryption key (TEK)

Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

traffic padding

The generation of spurious instances of communication, spurious data units, and/or spurious data within data units.

Source: ISO/IEC 7498-2

Note: May be used to disguise the amount of real data units being sent.

traffic flow security (TFS)

Techniques to counter Traffic Analysis.

training key

Key intended for use for over-the-air or off-the-air training.

Source: CNSSI No. 4005 (COMSEC)

transfer cross domain solution

A type of cross domain solution (CDS) that facilitates the movement of data between information systems operating in different security domains.

Source: DoDI 8540.01; CNSSI No. 1253F Attachment 3

transfer key encryption key (TrKEK)

A key used to move key from a Key Processor to a data transfer device (DTD)/secure DTD2000 system (SDS)/simple key loader (SKL).

Source: CNSSI No. 4005 (COMSEC)

transfer of accountability

The process of transferring accountability for COMSEC material from the COMSEC account of the shipping organization to the COMSEC account of the receiving organization.

Source: CNSSI No. 4005 (COMSEC); NSA/CSS Manual Number 3-16 (COMSEC)

transport layer security (TLS) protocol

A security protocol providing privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol.

Source: IETF RFC 5246 (adapted)

tranquility

Property whereby the security level of an object cannot change while the object is being processed by an information system.

transmission

The state that exists when information is being electronically sent from one location to one or more other locations.

transmission security (TRANSEC)

Measures (security controls) applied to transmissions in order to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals.

Note: TRANSEC is that field of COMSEC which deals with the security of communication transmissions, rather than that of the information being communicated.

trap door

1. A means of reading cryptographically protected information by the use of private knowledge of weaknesses in the cryptographic algorithm used to protect the data. See backdoor.

2. In cryptography, one-to-one function that is easy to compute in one direction, yet believed to be difficult to invert without special information.

trigger

1) <insider threat> A set of logic statements to be applied to a data stream that produces an alert when an anomalous incident or behavior occurs

Source - CNSSD No. 504 (2014)

2) An event that causes the system to initiate a response.

Note: Also known as triggering event.

Source: ISO/IEC 27031

triple data encryption algorithm (TDEA)

An approved cryptographic algorithm as required by FIPS PUB 140-2. TDEA specifies both the DEA cryptographic engine employed by TDEA and the TDEA algorithm itself.

Source: NIST SP 800-67 Rev 1 (adapted)

triple DES (3DES) (C.F.D.)

An implementation of the data encryption standard (DES) algorithm that uses three passes of the DES algorithm instead of one as used in ordinary DES applications. Triple DES provides much stronger encryption than ordinary DES but it is less secure than advanced encryption standard (AES).

Rationale: The terminology has been changed by NIST.

trojan horse

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

trust anchor

An established point of trust (usually based on the authority of some person, office, or organization) from which an entity begins the validation of an authorized process or authorized (signed) package. A "trust anchor" is sometimes defined as just a public key used for different purposes (e.g., validating a certification authority (CA), validating a signed software package or key, validating the process (or person) loading the signed software or key).

trust list

Collection of trusted certificates used by Relying Parties to authenticate other certificates.

Source: NIST SP 800-32

trusted agent (TA)

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

Source: CNSSI No. 1300

2. Entity authorized to act as a representative of an Agency in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.

Source: NIST SP 800-32

trusted certificate

A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a “trust anchor.”

Source: NIST SP 800-32

trusted channel

A channel where the endpoints are known and data integrity is protected in transit. Depending on the communications protocol used, data privacy may be protected in transit. Examples include transport layer security (TLS), IP security (IPSec), and secure physical connection.

trusted computer system

A system that has the necessary security functions and assurance that the security policy will be enforced and that can process a range of information sensitivities (i.e. classified, controlled unclassified information (CUI), or unclassified public information) simultaneously.

trusted computing base (TCB)

Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy.

trusted foundry

Facility that produces integrated circuits with a higher level of integrity assurance.

trusted operating system

An operating system in which there exists a level of confidence (based on rigorous analysis and testing) that the security principals and mechanisms (e.g., separation, isolation, least privilege, discretionary and non-discretionary access control, trusted path, authentication, and security policy enforcement) are correctly implemented and operate as intended even in the presence of adversarial activity.

Source: CNSSI No. 1253

trusted path

A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software.

Source: NIST SP 800-53 Rev 4

trusted process

Process that has been tested and verified to operate only as intended.

trusted recovery

Ability to ensure recovery without compromise after a system failure.

trusted timestamp

A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.

Source: NIST SP 800-32

trustworthiness

The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.

TSEC nomenclature

The NSA system for identifying the type and purpose of certain items of COMSEC material.

Source: CNSSI No. 4005 (COMSEC)

tunneling

Technology enabling one network to send its data via another network’s connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.

two-person control (TPC)

The continuous surveillance and control of material at all times by a minimum of two authorized individuals, each capable of detecting incorrect or unauthorized procedures with respect to the task being performed and each familiar with established security requirements.

Source: DoDI 5200.44

two-person integrity (TPI)

The system of storage and handling designed to prohibit individual access to certain COMSEC keying material by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

Note: Two-Person Control refers to the handling of Nuclear Command and Control COMSEC material while Two-Person Integrity refers only to the handling of COMSEC keying material.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

type accreditation (C.F.D.)

A form of accreditation that is used to authorize multiple instances of a major application or general support system for operation at approved locations with the same type of computing environment. In situations where a major application or general support system is installed at multiple locations, a type accreditation will satisfy Certification and Accreditation (C&A) requirements only if the application or system consists of a common set of tested and approved hardware, software, and firmware.

See type authorization.

type authorization

An official authorization decision to employ identical copies of an information system or subsystem (including hardware, software, firmware, and/or applications) in specified environments of operation.

Source: NIST SP 800-37 Rev. 1

type certification

The certification acceptance of replica information systems based on the comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made as part of and in support of the formal approval process, to establish the extent to which a particular design and implementation meet a specified set of security requirements.

U.S. national interests

Matters of vital interest to the United States to include national security, public safety, national economic security, the safe and reliable functioning of “critical infrastructure”, and the availability of “key resources”.

Source: PPD 20

U.S. person

U.S. person means a person (as defined in 22 CFR 120.14) who is a lawful permanent resident as defined by 8 U.S.C. 1101(a) (20) or who is a protected individual as defined by 8 U.S.C. 1324b(a) (3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the United States. It also includes any governmental (federal, state or local) entity. It does not include any foreign person as defined in 22 CFR 120.16.

Source: 22 CFR 120.15

U.S.-controlled facility

A base or building, access to which is physically controlled by U.S. citizens or resident aliens who are authorized U.S. Government or U.S. Government contractor employees.

Source: NSTISSI No. 3013

U.S.-controlled space

A space (e.g., room or floor) within a facility other than a U.S.-controlled facility, access to which is physically controlled by U.S. citizens or resident aliens who are authorized U.S. Government or U.S. Government contractor employees. Keys or combinations to locks controlling entrance to the U.S.-controlled space must be under the exclusive control of U.S. citizens or resident aliens who are U.S. Government or U.S. Government contractor employees.

Source: NTISSI 3013

unattended

A facility is unattended when there is no human presence. Use of roaming guards and/or an intrusion detection system is not enough to consider a facility attended. Having a trusted individual sitting at the entrance to a vault does make the vault attended.

Source: CNSSI No. 4005 (COMSEC)

unauthorized access

Any access that violates the stated security policy.

unauthorized disclosure

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

Source: NIST SP 800-57 Part 3

unclassified

Information that does not require safeguarding or dissemination controls pursuant to Executive Order (E.O.) 13556 (Controlled Unclassified Information) and has not been determined to require protection against unauthorized disclosure pursuant to E.O. 13526 (Classified National Security Information), or any predecessor or successor Order, or the Atomic Energy Act of 1954, as amended.

See controlled unclassified information (CUI), and classified national security information.

unencrypted key

Key that has not been encrypted in a system approved by the National Security Agency (NSA) for key encryption or encrypted key in the presence of its associated key encryption key (KEK) or transfer key encryption key (TrKEK). Encrypted key in the same fill device as its **associated** KEK or TrKEK is considered unencrypted. (Unencrypted key is also known as RED key).

Source: CNSSI No. 4005 (COMSEC)

unkeyed

COMSEC equipment containing no key or containing key that has been protected from unauthorized use by removing the cryptographic ignition key (CIK) or deactivating the personal identification number (PIN).

Source: CNSSI No. 4005 (COMSEC)

untrusted process

Process that has not been evaluated or examined for correctness and adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms.

update (a certificate)

1. The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.

Source: NIST SP 800-32

2. The process of creating a new certificate with a new serial number that differs in one or more fields from the old certificate. The new certificate may have the same or different subject public key.

Source: CNSSI No. 1300 (adapted from the word modification)

update (a key)

Automatic or manual cryptographic process that irreversibly modifies the state of a COMSEC key, equipment, device, or system.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

US-CERT (United States Computer Emergency Readiness Team)

A partnership between the Department of Homeland Security (DHS) and the public and private sectors, established to protect the nation's internet infrastructure. US-CERT coordinates defense against and responses to cyber attacks across the nation.

user

1. Individual, or (system) process acting on behalf of an individual, authorized to access an information system.

Source: NIST SP 800-53 Rev 4

2. An individual who is required to use COMSEC material in the performance of his/her official duties and who is responsible for safeguarding that COMSEC material. See hand receipt holder and local element.

Source: CNSSI No. 4005 (COMSEC); NSA/CSS Manual Number 3-16 (COMSEC)

user activity monitoring

The technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing U.S. Government information in order to detect insider threat and to support authorized investigations.

Source: CNSSD No. 504

user ID

Unique symbol or character string used by an information system to identify a specific user.

user representative (COMSEC)

The key management entity (KME) authorized by an organization and registered by the Central Facility Finksburg (CFFB) to order asymmetric key (including secure data network system (SDNS) key and message signature key (MSK)).

Source: CNSSI No. 4005 (COMSEC) (adapted)

user representative (risk management)

The person that defines the system’s operational and functional requirements, and who is responsible for ensuring that user operational interests are met throughout the systems authorization process.

validation

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

variant

One of two or more code symbols having the same plain text equivalent.

verification

Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome.

verifier

An entity that verifies the claimant's identity by verifying the claimant's possession and control of a token using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the token and identity and check their status.

Source: NIST SP 800-63-2

virtual private network (VPN)

Protected information system link utilizing tunneling, security controls (see information assurance (IA)), and endpoint address translation giving the impression of a dedicated line.

virus

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

voice over internet protocol (VoIP)

A term used to describe the transmission of packetized voice using the internet protocol (IP) and consists of both signaling and media protocols.

Source: CNSSI No. 5000

vulnerability

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

Source: NIST SP 800-30 Rev 1

vulnerability analysis

See vulnerability assessment.

Source: NIST IR 7298 Rev 2

vulnerability assessment

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

warm site

An environmentally conditioned work space that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption.

Source: NIST 800-34 Rev 1

watering hole attack

In a watering hole attack, the attacker compromises a site likely to be visited by a particular target group, rather than attacking the target group directly.

web bug

Malicious code, invisible to a user, placed on web sites in such a way that it allows third parties to track use of web servers and collect information about the user, including internet protocol (IP) address, host name, browser type and version, operating system name and version, and web browser cookie.

white list

A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or information system.

Also known as “clean word list”.

Source: NIST SP 800-128

whaling

A specific kind of phishing that targets high-ranking members of organizations.

White Team

1. The group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of their enterprise’s use of information systems. In an exercise, the White Team acts as the judges, enforces the rules of the exercise, observes the exercise, scores teams, resolves any problems that may arise, handles all requests for information or questions, and ensures that the competition runs fairly and does not cause operational problems for the defender's mission. The White Team helps to establish the rules of engagement, the metrics for assessing results and the procedures for providing operational security for the engagement. The White Team normally has responsibility for deriving lessons-learned, conducting the post engagement assessment, and promulgating results.

2. Can also refer to a small group of people who have prior knowledge of unannounced Red Team activities. The White Team acts as observers during the Red Team activity and ensures the scope of testing does not exceed a pre-defined threshold.

whitelisting

1). An approved list or register of entities that are provided a particular privilege, service, mobility, access or recognition.
2). An implementation of a default deny all or allow by exception policy across an enterprise environment, and a clear, concise, timely process for adding exceptions when required for mission accomplishments.

Source: CNSSI No. 1011

wi-fi protected access-2 (WPA2)

The approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. For federal government use, the implementation must use federal information processing standards (FIPS) approved encryption, such as advanced encryption standard (AES).

wireless intrusion detection system (WIDS)

A commercial wireless technology that assists designated personnel with the monitoring of specific parts of the radio frequency (RF) spectrum to identify unauthorized wireless transmissions and/or activities.

Source: DoD 8420.1

wireless access point (WAP)

A device that allows wireless devices to connect to a wired network using wi-fi, or related standards.

wireless application protocol (WAP)

A standard that defines the way in which Internet communications and other advanced services are provided on wireless mobile devices.

wireless technology

Technology that permits the transfer of information between separated points without physical connection.

Note: Currently wireless technologies use infrared, acoustic, radio frequency, and optical.

witness

An appropriately cleared (if applicable) and designated individual, other than the COMSEC Account Manager, who observes and testifies to the inventory or destruction of COMSEC material.

Source: CNSSI No. 4005 (COMSEC)

work factor

Estimate of the effort or time needed by a potential perpetrator, with specified expertise and resources, to overcome a protective measure.

workcraft identify

Synonymous with tradecraft identity.

worm

A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. See malicious code.

X.509 public key certificate

The public key for a user (or device) and a name for the user (or device), together with some other information, rendered unforgeable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard.

Source: NIST SP 800-57 Part 1 Rev 3 (adapted)

Also known as X.509 Certificate.

zero day attack

An attack that exploits a previously unknown hardware, firmware, or software vulnerability.

zero fill

To fill unused storage locations in an information system with a numeric value of zero.

zeroization

A method of erasing electronically stored data, cryptographic keys, and credentials service providers (CSPs) by altering or deleting the contents of the data storage to prevent recovery of the data.

Source: FIPS PUB 140-2

zeroize

To remove or eliminate the key from a cryptographic equipment or fill device.

Source: NSA/CSS Manual Number 3-16 (COMSEC)

zone of control

Three dimensional space surrounding equipment that processes classified and/or controlled unclassified information (CUI) within which TEMPEST exploitation is not considered practical or where legal authority to identify and remove a potential TEMPEST exploitation exists.

Annex A

Acronyms

Acronym	Expansion
ABAC	Attribute Based Access Control
ACD	Active Cyber Defense
ACL	Access Control List
ADP	Automatic Data Processing
AES	Advanced Encryption Standard
AKP	Advanced Key Processor
ALC	Accounting Legend Code
ANSI	American National Standards Institute
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
APT	Advanced Persistent Threat
APU	Auxiliary Power Unit
ARF	Asset Reporting Format
ASCII	American Standard Code for Information Interchange
ASIC	Application-Specific Integrated Circuit
AS&W	Attack Sensing and Warning
AT	Anti-tampering
ATC	Approval to Connect
ATM	Asynchronous Transfer Mode
ATO	1. Approval to Operate (C.F.D.) 2. Authorization to Operate
BoE	Body of Evidence
BCP	Business Continuity Plan
BIA	Business Impact Analysis

BMA	Business Mission Area
C2	Command and Control
C3	Command, Control, and Communications
C3I	Command, Control, Communications and Intelligence
C4	Command, Control, Communications and Computers
CA	1. Controlling Authority 2. Cryptanalysis 3. Certification Authority
C&A	Certification and Accreditation
CAC	Common Access Card
CAS	Certification Authority System
CAVP	Cryptographic Algorithm Validation Program
CAW (C.F.D.)	Certification Authority Workstation
CC	Common Criteria
CCB	Configuration Control Board
CCE	Common Configuration Enumeration
CCEB	Combined Communications-Electronics Board
CCEP	Commercial COMSEC Evaluation Program
CCEVS	Common Criteria Evaluation and Validation Scheme
CCI	1. Controlled Cryptographic Item 2. Control Correlation Identifier
CD	1. Compact Disc 2. Cross Domain
CDS	Cross Domain Solution
CERT	Computer Emergency Readiness Team
C.F.D.	Candidate for Deletion
CFD	Common Fill Device
CFFB	Central Facility Finksburg
CFR	Code of Federal Regulations
CHVP	Cryptographic High Value Products

CIK	Cryptographic Ignition Key
CIKR	Critical Infrastructure and Key Resources
CIMA	COMSEC Incident Monitoring Activity
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIRC	1. Computer Incident Response Center 2. Computer Incident Response Capability 3. Cyber Incident Response Team
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CKG	Cooperative Key Generation
CKL	Compromised Key List
CMCS	COMSEC Material Control System
CMDAUTH	Command Authority
CMVP	Cryptographic Module Validation Program
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CNSS	Committee on National Security Systems
CNSSAM	Committee on National Security Systems Advisory Memorandum
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CO	Cyberspace Operations
COA	Course of Action
COG	Continuity of Government
COI	Community of Interest
COMPUSEC (C.F.D.)	Computer Security

COMSEC	Communications Security
CONAUTH	Controlling Authority
CONOP	Concept of Operations
COOP	Continuity of Operations Plan
COR	1. Central Office of Record (COMSEC) 2. Contracting Officer Representative
COTS	Commercial off-the-shelf
CP	Certificate Policy
CPE	Common Platform Enumeration
CPS	Certification Practice Statement
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSA	Certificate Status Authority
CSfC	Commercial Solutions for Classified
CSIRT	Computer Security Incident Response Team
CSN	Central Services Node
CSO	Computer Security Object
CSP	Credentials Service Provider
CSS	1. Central Security Service 2. Certificate Status Server
CT1	Common Tier 1
CTAK	Cipher Text Auto-Key
CT&E	Certification Test and Evaluation
CTS	Computerized Telephone System
CTTA	Certified TEMPEST Technical Authority
CUAS	Common User Application Software
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures

CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CybOX	Cyber Observable eXpression
D/A	Department/Agency
D/S	Directory Service
DAA	1. Designated Accrediting Authority 2. Designated Approval Authority (C.F.D.)
DAC	Discretionary Access Control
DAR	Data-at-Rest
DC3	Defense Cyber Crime Center
DCID	Director Central Intelligence Directive
DCO	Defensive Cyberspace Operations
DCO-RA	Defensive Cyberspace Operation Response Action
DCS	1. Defense Courier Service 2. Distributed Control System
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DIACAP (C.F.D.)	DoD Information Assurance Certification and Accreditation Process
DIMA	DoD portion of the Intelligence Mission Area
DISN	Defense Information System Network
DIT	Data in Transit
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMZ	Demilitarized Zone
DN	Distinguished Name
DOC (C.F.D.)	Delivery-Only Client
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDM	Department of Defense Manual

DoDIN	Department of Defense Information Networks
DoS	Denial of Service
DRP	Disaster Recovery Plan
DSOC	DoD Strategy for Operating in Cyberspace
DTD	Data Transfer Device
EA	Enterprise Architecture
EAL (C.F.D.)	Evaluation Assurance Level
EAP	Emergency Action Plan
ECCM	Electronic Counter-Countermeasures
ECDS	Enterprise Cross Domain Services
ECM	Electronic Countermeasures
ECU	End Cryptographic Unit
EFD	Electronic Fill Device
EIEMA	Enterprise Information Environment Mission Area
EIRP	Effective Isotropic Radiated Power
EKMS	Electronic Key Management System
EMSEC	Emission Security
E.O.	Executive Order
EPL (C.F.D.)	Evaluated Products List
EPROM	Erasable, Programmable, Read-Only Memory
ERTZ	Equipment Radiation TEMPEST Zone
ESSA	Enhanced Shared Situational Awareness
ETPL	Endorsed TEMPEST Products List
FAR	False Accept Rate
FBCA	Federal Bridge Certification Authority
FEA	Federal Enterprise Architecture
FICAM	Federated Identity, Credential and Access Management
FIPS	Federal Information Processing Standards

FISMA	Federal Information Security Management Act
FOCI	Foreign Owned, Controlled or Influenced
FOUO	For Official Use Only
FRR	False Reject Rate
FTR	Field Tamper Recovery
GCA	Government Contracting Activity
GIG (C.F.D.)	Global Information Grid
GOTS	Government-off-the-Shelf
GSS	General Support System
HAIPE	High Assurance Internet Protocol Encryptor
HMAC	Hash- Based Message Authentication Code
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
I&A	Identification and Authentication
IaaS	Infrastructure as a Service
IAB	Internet Architecture Board
IAC	Information Assurance Component
IAM (C.F.D.)	Information Assurance Manager
IAO (C.F.D.)	Information Assurance Officer
IASAE	Information Assurance Workforce System Architecture
IATO (C.F.D.)	Interim Approval to Operate
IATT	Interim Authorization to Test
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IBAC	Identity Based Access Control
IC	Intelligence Community
ICAM	Identity, Credential and Access Management

ICANN	Internet Corporation for Assigned Names and Numbers
ICD	Intelligence Community Directive
ICS	1. Intelligence Community Standard 2. Industrial Control System
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
INFOSEC	Information Systems Security
IO	Information Operations
IP	Internet Protocol
IPSec	IP Security
IR	Interagency Report
IRM	Information Resources Management
IS	Information System
ISA	1. Interconnection Security Agreement 2. Information Sharing Architecture
ISCM	Information Security Continuous Monitoring
ISE	Information Sharing Environment
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISSE	Information Systems Security Engineer/Engineering
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
ITAR	International Traffic in Arms Regulation
IV	Initialization Vector
IVA	Independent Validation Authority
IV&V	Independent Verification and Validation
JP	Joint Publication

KAK	Key-Auto-Key
KDC	Key Distribution Center
KEK	Key Encryption Key
KG	Key Generator
KMC	Key Management Center
KME	Key Management Entity
KMI	Key Management Infrastructure
KMID	Key Management Identification Number
KMP	1. Key Management Protocol 2. Key Management Plan
KMS	Key Management System
KOA	KMI Operating Account
KOAM	KMI Operating Account Manager
KP	Key Processor
KPC	KMI Protected Channel
KSD	Key Storage Device
LAN	Local Area Network
LCMS	Local COMSEC Management Software
LMD	Local Management Device
LMD/KP	Local Management Device/Key Processor
LPD	Low Probability of Detection
LPI	Low Probability of Intercept
LRA	Local Registration Authority
LRIP	Low Rate Initial Production
LSI	Large Scale Integration
MAC	1. Mandatory Access Control 2. Message Authentication Code 3. Mission Assurance Category (C.F.D.)
MAN	1. Mandatory Modification 2. Metropolitan Area Network

MGC	Management Client
MI	Message Indicator
MIME	Multipurpose Internet Mail Extensions
MitM	Man-in-the-Middle Attack
MLS	Multilevel Security
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSK	Message Signature Key
MSL	Multiple Security Levels
NACAM	National COMSEC Advisory Memorandum
NACSI	National COMSEC Instruction
NACSIM	National COMSEC Information Memorandum
NAK	Negative Acknowledgement
NCIRS	National COMSEC Incident Reporting System
NIAP	National Information Assurance Partnership
NID	National Interest Determination
NII	National Information Infrastructure
NIST	National Institute of Standards and Technology
NLZ	No-Lone Zone
NPE	Non-Person Entity
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSD	National Security Directive
NSDD	National Security Decision Directive
NSI	National Security Information
NSS	National Security System
NSTAC	National Security Telecommunications Advisory Committee

NSTISSAM	National Security Telecommunications and Information Systems Security Advisory/Information Memorandum
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSD	National Security Telecommunications and Information Systems Security Directive
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NTISSAM	National Telecommunications and Information Systems Security Advisory/Information Memorandum
NTISSD	National Telecommunications and Information Systems Security Directive
NTISSI	National Telecommunications and Information Systems Security Instruction
NTISSP	National Telecommunications and Information Systems Security Policy
NVD	National Vulnerability Database
OADR	Originating Agency's Determination Required
OCO	Offensive Cyberspace Operations
OMB	Office of Management and Budget
OPCODE	Operations Code
OPM	Ordering Privilege Manager
OPSEC	Operations Security
ORA	Organizational Registration Authority
OSI	Open Systems Interconnection
OTAD	Over-the-Air Key Distribution
OTAR	Over-the-Air Rekeying
OTAT	Over-the-Air Key Transfer
OTP	One-Time Pad
OTT	One-Time Tape
OVAL	Open Vulnerability Assessment Language
PAA (C.F.D.)	(IC) Principal Accrediting Authority

PaaS	Platform as a Service
PAO	Principal Authorizing Official
PBAC	Policy Based Access Control
PBX	Private Branch Exchange
PCL	Product Compliant List
PCM	Privilege Certificate Manager or Positive Control Material
PCMCIA	Personal Computer Memory Card International Association
PDP	Policy Decision Point
PDR	Preliminary Design Review
PDS	Protected Distribution System
PED	Portable Electronic Device
PEP	Policy Enforcement Point
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIT	Platform Information Technology
PIV	Personal Identity Verification
PKC	Public Key Cryptography
PKE	Public Key Enabling
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
POA&M	Plan of Action and Milestones
PPD	Presidential Policy Directive
PPS	Physically Protected Space
PRM	Performance Reference Model
PRNG	Pseudorandom Number Generator
PROM	Programmable Read-Only Memory
PROPIN	Proprietary Information

PRSN	Primary Services Node
PSN	Product Source Node
PWA	Printed Wiring Assembly
RA	Registration Authority
RAdAC	Risk Adaptable Access Control
RBAC	Role Based Access Control
RD	Restricted Data
RF	Radio Frequency
RMF	Risk Management Framework
RNG	Random Number Generator
ROM	Read-Only Memory
RVTM	Requirements Verification Traceability Matrix
SA	1. System Administrator 2. Situational Awareness
SaaS	Software as a Service
SABI	Secret and Below Interoperability
SAISO	Senior Agency Information Security Officer
SAML	Security Assertion Markup Language
SAP	Special Access Program
SAPF	Special Access Program Facility
SAR	Security Assessment Report
SBU	Sensitive But Unclassified
SCA	Security Control Assessor
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCIP	Secure Communications Interoperability Protocol

SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SDR	System Design Review
SDS	Secure DTD2000 System
SED	1. Self-Encrypting Devices 2. Self-Encrypting Drives
SFA	Security Fault Analysis
SHA	Secure Hash Algorithm
SFUG (C.F.D.)	Security Features Users Guide
SIAO (C.F.D.)	Senior Information Assurance Officer
SISO	Senior Information Security Officer
SKL	Simple Key Loader
SLA	Service Level Agreement
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SoM	Strength of Mechanism
SOP	Standard Operating Procedure
SP	Special Publication
SPK	Single Point Key(ing)
SRG	Security Requirements Guide
SRR	Security/System Requirements Review
SRTM	Security Requirements Traceability Matrix
SSA	Shared Situational Awareness
SSAA	System Security Authorization Agreement
SSL	Secure Socket Layer
SSO	Systems Security Officer
SSP	System Security Plan
ST&E	Security Test and Evaluation

STAR	Short Title Assignment Requester
STE	Secure Terminal Equipment
STIG	Security Technical Implementation Guide
STIX	Structured Threat Information eXpression
STU	Secure Telephone Unit
SwA	Software Assurance
SWID	Software Identification
TA	1. Traffic Analysis 2. Trusted Agent
TAG	TEMPEST Advisory Group
TAXII	Trusted Automated eXchange of Indicator Information
TCB	Trusted Computing Base
TCP/IP	Transmission Control Protocol/Internet Protocol
TDEA	Triple Data Encryption Algorithm
TEK	Traffic Encryption Key
TFS	Traffic Flow Security
TLS	Transport Layer Security
TOE	Target of Evaluation
TPC	Two-Person Control
TPI	Two-Person Integrity
TRANSEC	Transmission Security
TRB	Technical Review Board
TrKEK	Transfer Key Encryption Key
TRM	Technical Reference Model
TSCM	Technical Surveillance Countermeasures
TSEC	Telecommunications Security
TTP	Tactics, Techniques and Procedures
UAS	User Applications Software

UCDSMO	Unified Cross Domain Services Management Office
UIS	User Interface System
URL	Universal Resource Locators
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
USC	United States Code
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	1. Wireless Access Point 2. Wireless Application Protocol
WEP	Wired Equivalent Privacy
WG	Working Group
WIDS	Wireless Intrusion Detection System
WLAN	Wireless Local Area Network
WMA	Warfighting Mission Area
WPA2	Wi-Fi Protected Access - 2
XCCDF	eXtensible Configuration Checklist Description Format
XML	Extensible Markup Language

Annex B

References

The following documents were used in whole or in part as background material in development of this instruction:

1. P. Bourque and R.E. Fairley, eds., *Guide to the Software Engineering Body of Knowledge*, Version 3.0, IEEE Computer Society, 2014.
2. Chairman of the Joint Chiefs of Staff 6211.02D, *Defense Information Systems Network (DISN) Responsibilities*, January 2012.
3. Committee on National Security Systems Advisory Memoranda (CNSSAM) TEMPEST/1-13 *RED/BLACK Installation Guidance*, January 2014.
4. Committee on National Security Systems Advisory Memoranda (CNSSAM) Information Assurance (IA)/01-12 6 Jun 12 *NSA-Approved Commercial Solution Guidance*, June 2012.
5. Committee on National Security Systems Directive (CNSSD) No. 502, *National Directive on Security of National Security Systems*, December 2004.
6. Committee on National Security Systems Directive (CNSSD) No. 504, *Directive on Protecting NSS from Insider Threat*, February 2014.
7. Committee on National Security Systems Directive (CNSSD) No. 505, *Supply Chain Risk Management (SCRM)*, March 2012.
8. Committee on National Security Systems Directive (CNSSD) No. 506, *Implement Public Key Infrastructure for the Protection of Systems Operating on Secret Level Networks*, October 2012.
9. Committee on National Security Systems Directive (CNSSD) No. 507, *National Directive for Identity, Credential, and Access Management Capabilities (ICAM) on the United States (US) Federal Secret Fabric*, January 2014.
10. Committee on National Security Systems Instruction (CNSSI) No. 1011, *Implementing Host-Based Security Capabilities on National Security Systems*, July 2013.
11. Committee on National Security Systems Instruction (CNSSI) No. 1012, *Instruction for Network Mapping of National Security Systems (NSS)*, July 2013.
12. Committee on National Security Systems Instruction (CNSSI) No. 1013, *Network Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS) on National Security Systems*, July 2013.
13. Committee on National Security Systems Instruction (CNSSI) No. 1200, *National Information Assurance Instruction for Space Systems used to Support National Security Missions*, May 2014.

14. Committee on National Security Systems Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection for National Security Systems*, March 2014.

15. Committee on National Security Systems Instruction (CNSSI) No. 1253F Attachment 3, *Cross Domain Solution Overlay*, September 2013.

16. Committee on National Security Systems Instruction (CNSSI) No. 1300, *National Instruction On Public Key Infrastructure X.509 Certificate Policy, Under CNSS Policy No. 25*, September 2013.

17. Committee on National Security Systems Instruction (CNSSI) No. 4001, *Controlled Cryptographic Items*, May 2013.

18. Committee on National Security Systems Instruction (CNSSI) No. 4003, *Reporting and Evaluating COMSEC Incidents*, May 2014.

19. Committee on National Security Systems Instruction (CNSSI) No. 4005, *Safeguarding COMSEC Facilities and Materials*, August 2011.

20. Committee on National Security Systems Instruction (CNSSI) No. 4006, *Controlling Authorities for Traditional COMSEC Keying Material*, December 2012.

21. Committee on National Security Systems Instruction (CNSSI) No. 4009, *National Information Assurance Glossary*, April 2010.

22. Committee on National Security Systems Instruction (CNSSI) No. 4014, *Information Systems Security Officers National Information Assurance Training Standard*, April 2004.

23. Committee on National Security Systems Instruction (CNSSI) No. 4016, *National Information Assurance Training Standard for Risk Analysts*, November 2005.

24. Committee on National Security Systems Instruction (CNSSI) No. 4032, Title not available, December 2012.

25. Committee on National Security Systems Instruction (CNSSI) No. 4033, Nomenclature for Communications Security Material, November 2012.

26. Committee on National Security Systems Instruction (CNSSI) No. 4004.1, *Destruction and Emergency Protection Procedures for COMSEC and Classified Material*, January 2008.

27. Committee on National Security Systems Instruction (CNSSI) No. 4032, Title not available, June 2012.

28. Committee on National Security Systems Instruction (CNSSI) No. 4033, *Nomenclature for Communications Security Material*, November 2012.

29. Committee on National Security Systems Instruction (CNSSI) No. 5002, *National Information Assurance (IA) Instruction for Computerized Telephone Systems*, February 2012.

30. Committee on National Security Systems Policy (CNSSP) No. 8, *Release and Transfer of U.S. Government (USG) Cryptologic National Security Systems Technical Security Material,*

Information, and Techniques to Foreign Governments and International Organizations, August 2012.

31. Committee on National Security Systems Policy (CNSSP) No. 11, *Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, June 2013.
32. Committee on National Security Systems Policy (CNSSP) No. 15, *National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems*, October 2012.
33. Committee on National Security Systems Policy (CNSSP) No. 19, *National Policy Governing the Use of High Assurance Internet Protocol Encryptor (HAIPE)*, June 2013.
34. Committee on National Security Systems Policy (CNSSP) No. 24, *Policy on Assured Information Sharing (AIS) for National Security Systems (NSS)*, May 2010.
35. Common Criteria Maintenance Board (CCMB)-2012-09-003, *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 4, September 2012.
36. Defense Security Service (DSS) Center for Development of Security Excellence (CDSE), *Glossary of Security Terms, Definitions, and Acronyms*, November 2012.
37. Department of Defense (DoD) Biometrics Enterprise Architecture (Integrated) v2.0, *Common Biometric Vocabulary (CBV)*, April 2013.
38. Department of Defense (DoD) 4140.1-R, *DoD Supply Chain Materiel Management Regulation*, May 2003.
39. Department of Defense Directive (DoDD) 5230.09, *Clearance of DoD Information for Public Release*, August 2008.
40. Department of Defense Directive (DoDD) 5505.13E, *DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)*, March 2010.
41. Department of Defense Directive (DoDD) 8570.01, *Information Assurance Training, Certification, and Workforce Management*, August 2004.
42. Department of Defense Instruction (DoDI) 1000.13, *Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals,* January 2014.
43. Department of Defense Instruction (DoDI) 4000.19, *Support Agreements,* April 2013.
44. Department of Defense Instruction (DoDI) 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense,* December 2010.
45. Department of Defense Instruction (DoDI) 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, November 2012.
46. Department of Defense Instruction (DoDI) 5240.05, *Technical Surveillance Countermeasures (TSCM)*, April 2014.

47. Department of Defense Instruction (DoDI) 8115.02, *Information Technology Portfolio Management Implementation,* October 2006.
48. Department of Defense Instruction (DoDI) 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies,* November 2009.
49. Department of Defense Instruction (DoDI) 8500.01, *Cybersecurity,* March 2014.
50. Department of Defense Instruction (DoDI) 8500.2, *Information Assurance Implementation*, February 2003.
51. Department of Defense Instruction (DoDI) 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, March 2014.
52. Department of Defense Instruction (DoDI) 8540.01, *Cross Domain (CD) Policy*, DRAFT.
53. Department of Defense Manual (DoDM) 5200.01, Volume 4, *DoD Information Security Program: Controlled Unclassified Information (CUI)*, February 2012.
54. Department of Defense Manual (DoDM) 5205.07, Volume 4, *Special Access Program (SAP) Security Manual: Marking*, October 2013.
55. Department of Defense Manual (DoDM) 5220.22, Volume 3, *National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)*, April 2014.
56. Department of Defense Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, November 2010.
57. Department of Defense Joint Publication (JP) 3-12, *Joint Cyberspace Operations*, February 2013.
58. Department of Defense Joint Publication (JP) 6-0, *Joint Communications System*, June 2010.
59. Department of Homeland Security Office of Inspector General (OIG) 11-121, *Management Advisory Report on Cybersecurity*, September 2011.
60. Department of Homeland Security, *Information Technology Sector Baseline Risk Assessment*, August 2009.
61. Department of Justice, *Report on Phishing*, October 2006.
62. Executive Order (E.O.) 12333, as amended, *United States Intelligence Activities*, December 1981.
63. Executive Order (E.O.) 13231, *Critical Infrastructure Protection in the Information Age,* October 2001.
64. Executive Order (E.O.)13292, *Further Amendment to Executive Order 12958, as Amended, Classified National Security Information*, March 2003.
65. Executive Order (E.O.) 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, October 2005.
66. Executive Order (E.O.) 13526, *Classified National Security Information,* December 2009.

67. Executive Order (E.O.) 13556, *Controlled Unclassified Information*, November 2010.

68. *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, Version 2.0, December 2011.

69. Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001.

70. Federal Information Processing Standard (FIPS) Publication 180-4, *Secure Hash Standard (SHS)*, March 2012.

71. Federal Information Processing Standard (FIPS) Publication 186-4, *Digital Signature Standard (DSS)*, July 2013.

72. Federal Information Processing Standard (FIPS) Publication 188, *Standard Security Label for Information Transfer*, September 1994.

73. Federal Information Processing Standard (FIPS) Publication 197, *Advanced Encryption Standard (AES)*, November 2001.

74. Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

75. Federal Information Processing Standard (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

76. Federal Information Processing Standard (FIPS) Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006.

77. Information Sharing Architecture (ISA) Shared Situational Awareness (SSA), *Requirements Document*, version 2.1, October 2013.

78. Institute of Electrical and Electronics Engineers (IEEE) Computer Society, *Guide to the Software Engineering Body of Knowledge*, March 2005.

79. Intelligence Community Directive (ICD) No. 503, *Information Technology Systems Security Risk Management, Certification and Accreditation*, September 2008.

80. Intelligence Community Directive (ICD) No. 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented*, June 2013.

81. Intelligence Community Directive (ICD) No. 705, *Sensitive Compartmented Intelligence Facilities*, May 2010.

82. Intelligence Community Standard (ICS) 500-31, *Operating Cross Domain Solutions on the Intelligence Community Information Environment*, DRAFT.

83. Intelligence Community Standard (ICS) 700-1, *Glossary of Security Terms, Definitions, and Acronyms*, April 2008.

84. Intelligence Community Technical Specification (ICTS), Unified Identity Attribute Set (UIAS) v2, *IC Enterprise Attribute Exchange between IC Attribute Services Unified Identity Attribute Set*, July 2012.

85. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 7498-2:1989, *Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture*, 1989.

86. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15408-1:2009, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*, 2014.

87. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 19790:2006, *Information technology -- Security techniques -- Security requirements for cryptographic modules*, 2006.

88. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 19795-6:2012, *Information technology -- Biometric performance testing and reporting -- Part 6: Testing methodologies for operational evaluation*, 2012.

89. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000:2014, *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*, 2014.

90. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27031:2011, *Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity*, 2011.

91. Internet Engineering Task Force (IETF) Request for Comments (RFC) 4301, *Security Architecture for the Internet Protocol*, December 2005.

92. Internet Engineering Task Force (IETF) Request for Comments (RFC) 4949 Version 2, *Internet Security Glossary*, August 2007.

93. Internet Engineering Task Force (IETF) Request for Comments (RFC) 5246, *The Transport Layer Security (TLS) Protocol*, Version 1.2, August 2008.

94. National Aeronautics and Space Administration (NASA) Technical Standard (NASA-STD) 8739.8 w/Change 1, *Software Assurance Standard*, November 1992.

95. National Institute of Standards and Technology (NIST) Certificate Policy (CP)-1, *Certificate Policy CP-1 for FMS Public Key Certificates in Unclassified Environments*, DRAFT.

96. National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) Bulletin, *The National Vulnerability Database (NVD): Overview*, December 2013.

97. National Institute of Standards and Technology (NIST) Interagency Report (IR) 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*, October 2012.

98. National Institute of Standards and Technology (NIST) Interagency Report (IR) 7657, *A Report on the Privilege (Access) Management Workshop*, March 2010.

99. National Institute of Standards and Technology (NIST) Interagency Report (IR) 7298 Rev 2, *Glossary of Key Information Security Terms*, April 2006.

100. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

101. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18 Rev 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

102. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-21 2nd edition, *Guideline for Implementing Cryptography in the Federal Government*, December 2005.

103. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-27 Rev A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2004.

104. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-28, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001.

105. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Rev 1, *Risk Management*, September 2012.

106. National Institute of Standards and Technology (NIST) Special Publication (SP), 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001.

107. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34 Rev 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.

108. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Rev 1, *Guide for the Security Authorization of Federal Information Systems*, 2010.

109. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.

110. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-41 Rev 1, *Guidelines on Firewalls and Firewall Policy*, September 2009.

111. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-45 Version 2, *Guidelines on Electronic Mail Security*, February 2007.

112. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

113. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

114. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A Rev 1 Rev 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, June 2010.

115. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*, August 2009.

116. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-57 Part 1, *Recommendation for Key Management: Part 1: General (Revision 3)*, July 2012.

117. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-57 Part 3, *Recommendation for Key Management, Part 3 Application-Specific Key Management Guidance*, December 2009.

118. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

119. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 Rev 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.

120. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev 2, *Computer Security Incident Handling Guide*, August 2012.

121. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-2, *Electronic Authentication Guideline*, August 2013.

122. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-67 Rev 1, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, January 2012.

123. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-72, *Guidelines on PDA Forensics*, November 2004.

124. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007.

125. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 Rev 1, *Guide to Industrial Control Systems (ICS) Security*, April 2013.

126. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88 Rev 1, *Guidelines for Media Sanitization*, September 2012, DRAFT.

127. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007.

128. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

129. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-107 Rev 1, *Recommendation for Applications Using Approved Hash Algorithms*, August 2012.

130. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-124 Rev 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, June 2013.

131. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0*, November 2009.

132. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011.

133. National Security Agency (NSA) NAG-16F, *Field Generation and Over-The-Air Distribution of COMSEC Key in Support of Tactical Operations and Exercises*, May 2001.

134. National Security Agency/Central Security Service (NSA/CSS) Information Assurance Directorate (IAD) Guidance No. 400, *Retention of IA Mission Data*, December 2011.

135. National Security Agency/Central Security Service (NSA/CSS) Policy 11-1, *Information Sharing*, March 2012.

136. National Security Agency/Central Security Service (NSA/CSS) Policy 3-12, *Protected Distribution Systems for COMINT*, December 2014.

137. National Security Agency/Central Security Service (NSA/CSS) Policy 3-14, *NSA/CSS Certification and Approval for Use of Information Assurance Products and Solutions*, November 2013.

138. National Security Agency/Central Security Service (NSA/CSS) Policy Manual Number 3-16, *Control of Communications Security (COMSEC) Material*, August 2005.

139. National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, July 1990.

140. National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23, *Cybersecurity Policy*, January 2008.

141. National Security Telecommunications and Information Systems Security Directive (NSTISSD) 501, *National Security Program for Information Systems Security (INFOSEC) Professionals*, November 1992.

142. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7002, *TEMPEST Glossary*, March 1995.

143. National Security Telecommunications and Information Systems Security Directive (NSTISSD) 501, *National Training Program for Information Systems Security (INFOSEC) Professionals*, November 1992.

144. National Security Telecommunications and Information Systems Security Directive (NSTISSD) 600, *Communications Security Monitoring,* April 1990.

145. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 3006, *Operational Security Doctrine for the NAVSTAR Global Positioning System (GPS) Precise Positioning Service (PPS) User Segment Equipment,* August 2001.

146. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 3013, *Operational Security Doctrine for the Secure Telephone Unit III (STU-III) Type 1 Terminal,* February 1990.

147. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7002(TEMPEST), *TEMPEST Glossary,* March 1995.

148. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, *Protective Distribution Systems (PDS)*, December 1996.

149. National Telecommunications and Information Security System Policy (NTISSP) 200, *National Policy on Controlled Access Protection*, July 1987.

150. Office of Management and Budget (OMB) Transmittal Memorandum No. 4, Circular A-130, *Management of Federal Information Resources*, November 2000.

151. Official (ISC)^2® guide to the CISSP® CBK®: (ISC)^2® Press / Harold F. Tipton, Kevin Henry.

152. Presidential Policy Directive (PPD)-20, *U.S. Cyber Operations Policy*, October 2012.

153. Presidential Policy Directive (PPD)-21, *Critical Infrastructure Security and Resilience*, February 2013.

154. Public Law 104-106, *Clinger-Cohen Act of 1996*, January 1996.

155. Public Law 107-347 [H.R. 2458], *The E-Government Act of 2002, Title III, the Federal Information Security Management Act of 2002 (FISMA)*, December 2002.

156. Public Law 108-458, *Intelligence Reform and Terrorism Prevention Act of 2004*, December 2004.

157. RFC 4949, *Internet Security Glossary*, Version 2, August 2007.

158. Secretary of the Navy (SECNAV) M-5239.1, *Department of the Navy Information Assurance Program Information Assurance Manual*, November 2005.

159. United States Department of Commerce (USDC), *Defense Industrial Base Assessment: Counterfeit Electronics*, January 2010.

160. 22 Code of Federal Regulations (CFR) 120.15, *U.S. Person*, April 2011.

161. 32 Code of Federal Regulations (CFR) Part 2002, *Controlled Unclassified Information*, Draft as of October 21, 2014.

162. 40 United States Code (U.S.C.) Sec. 11101, *Definitions*, January 2012.

163. 40 United States Code (U.S.C.) Sec. 1401, *Definitions*, January 1999.

164. 40 United States Code (U.S.C.) Sec. 1425, *Agency Chief Information Officer*, January 2002.

165. 40 United States Code (U.S.C.) Sec 11331, *Responsibilities for Federal information systems standards*, February 2010.

166. 41 United States Code (U.S.C.) Sec. 403, *Definitions*, January 1995.

167. 44 United States Code (U.S.C.) Sec 3502, *Definitions*, January 2012.

168. 44 United States Code (U.S.C.) Sec 3542, *Definitions*, January 2012.

169. 44 United States Code (U.S.C.) Sec 3544, *Federal Agency Responsibilities*, January 2009.

170. 47 Code of Federal Regulations (CFR) Part 64 Appendix A, *Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NSEP)*, November 2006.

171. 50 United States Code (U.S.C.) Sec 3003, *Definitions*, January 2012.