Committee on National Security Systems

CNSSI 4009
March 2, 2022

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 2015. This revision of CNSSI No. 4009 incorporates many new terms submitted by the CNSS Membership. Most of the terms from the 2015 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 definitions also provides context and a reference for additional information.
   - 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, shown in italics (e.g., See *assurance*).
   - 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 200 in the current version. References not used as the source of terms and definitions were removed.

3. The glossary still contains definitions where sources are not specified. For these terms, definitions will be considered organic. These new terms are often emerging terms judged to be valuable to include in the glossary, but have not yet been defined in a published authoritative source, or terms where an adequate original definition source could not be identified.

4. Some definitions originate from an obsolete, withdrawn, or superseded source. In most cases, terms with no alternative definitions were found to be obsolete and deleted. In cases

where the term was deemed relevant, but no current authoritative source could be found, the obsolete source is shown as italicized and with an asterisk (e.g., **NCSC-TG-004*) in the table and labeled as withdrawn or superseded in the reference section. This allows for easier tracking of the etymology of a term and for understanding context.

5. Some sources list a given document and then note "(adapted)"—for example, the term "acquisition" states as its source "NSA/CSS Policy 3-4 (adapted)." "Adapted" indicates a definition derived from a source, but not verbatim from that source. An adapted definition given in CNSSI 4009 may be truncated from the original source's definition because of extraneous information, or it may be re-worded for clarity or accuracy, or it may be constructed using content from the original source (e.g., defining Controlled Cryptographic Item by using material from CNSSI No. 4001 and citing "CNSSI No. 4001 (adapted)" as the source).

6. 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 cybersecurity (CS) 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 the intended audience.

7. 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.

8. 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 either because they are still used in certain communities, or to provide users with traceability to the newer terms.

9. The format of the glossary has been updated from previous versions. This format allows an easier distinction between definitions with notes, notes added for this glossary, and multiple definitions from different sources (listed in alphabetical order). Context was also added to many terms and is shown in brackets (e.g., assessment [general context]). In addition, throughout the glossary, references to similar or updated terms are made. When that term exists in this document, it is italicized (e.g. See *assurance*); when the term is not in this document, it is put into quotes (e.g., Also known as "assurance").

10. 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 CS community.

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

FOR THE NATIONAL MANAGER:

/s/

ROBERT E. JOYCE
Deputy National Manager for National Security Systems

CNSS Secretariat (C07). National Security Agency. 9800 Savage Road, STE 6165. Ft Meade, MD 20755-6716
Office Phone Number: (410) 854-6805; Unclassified FAX Number: (410) 854-6814
CNSS@nsa.gov

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

Committee on National Security Systems (CNSS) 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	Source
access	Ability to make use of any information system (IS) resource.	NIST SP 800-32
	To make contact with one or more discrete functions of an online, digital service.	NIST SP 800-63-3
access and amendment [privacy context]	A privacy principle (FIPP) that refers to an organization's requirements to provide individuals with appropriate access to personally identifiable information (PII) and appropriate opportunity to correct or amend PII.	OMB Circular A-130 (adapted)
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) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).	FIPS 201-2

	The decision to permit or deny a subject access to system objects (network, data, application, service, etc.) See also *authorization*.	NIST SP 800-162 (adapted)
access control list (ACL)	A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity.	IETF RFC 4949 Ver 2
access control mechanism	As an implementation of formal access control policy based on a formal access control model, this is the logical component that serves to receive the access request from the subject, to decide, and to enforce the access decision. Access control mechanisms can be designed to adhere to the properties of the model by machine implementation using protocols, architecture, or formal languages such as program code.	NIST SP 800-162 and NIST SP 800-192 (adapted)

	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.	**NCSC-TG-004*
access cross domain solution	A type of transfer cross domain solution (CDS) that provides access to a computing platform, application, or data residing in different security domains without transfer of user data between the domains. Note: The access function is implemented by transferring keyboard and mouse data down to the lower security domain and sending video/image data up to the higher security domain.	CNSSI No. 1253F Attachment 3 (adapted)
access level	A category within a given security classification limiting entry or system connectivity to only authorized persons.	
access list	A list of users, programs, and/or processes and the specifications of access categories to which each is assigned.	**NCSC-TG-004*
	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.	
	The nature of an access right to a particular device, program, or file (e.g., read, write, execute, append, modify, delete, or create).	**NCSC-TG-004*

accountability [cryptographic context]	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.	CNSSI No. 4005
accountability [general context]	Property that ensures that the actions of an entity may be traced uniquely to the entity.	ISO/IEC 7498-2:1989
accountability [privacy context]	A privacy principle (FIPP) that refers to an organization's requirements to demonstrate their implementation of the FIPPs and applicable privacy requirements.	OMB Circular A-130 (adapted)
accountability [systems security context]	The security objective 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.	**NIST SP 800-33 (adapted)*
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).	CNSSI No. 4005
accounting number	A number assigned to an individual item of COMSEC material at its point of origin to facilitate its handling and accounting.	
accreditation [information security context] (C.F.D.)	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.	FIPS 200
	See *authorization to operate (ATO)*.	
	Note: For the information security context, this term was replaced in 2010 by the term *authorization*, but it is still seen occasionally in contracts and in organizations that rely on FIPS 200.	

	C.F.D. Rationale: The Risk Management Framework uses the term *authorization*, but FIPS 200 and other documents still use the term *accreditation*.	
accreditation [testing & evaluation context]	Formal recognition that a laboratory is competent to carry out specific tests or calibrations or types of tests or calibrations.	NIST Handbook 150; NIST NVLAP
acquirer	Stakeholder that acquires or procures a product or service.	NIST SP 800-161; ISO/IEC 15288:2015 (adapted)
acquisition	The process associated with obtaining products or services, typically through contracts involving the expenditure of financial resources, as well as to products or services that may be obtained on a cost-free basis via other mechanisms (e.g., the downloading of public domain software products and other software products with limited or no warranty, such as those commonly known as freeware or shareware from the commercial Internet).	NSA/CSS Policy 3-4 (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.	CNSSI No. 1300
active attack	An attack on a secure communication protocol where the attacker transmits data to the claimant, Credential Service Provider (CSP), verifier, or Relying Party (RP). Examples of active attacks include man-in-the middle (MitM), impersonation, and session hijacking.	NIST SP 800-63-3 (adapted)

	NIST SP 800-30 Rev. 1, Appendix E provides a representative list of threat events, including attacks. Active and passive attacks may include: Denial of Service (DoS); Distributed Denial of Service (DDoS); Cross-site Request Forgery (CSRF); Cross-site Scripting (XSS); manipulative communications deception; phishing; laboratory attacks; side channel attacks; spear phishing; whaling; and Trojan Horses. See also *passive attack*	
active content	Electronic documents that can carry out or trigger actions automatically on a computer platform without the intervention of a user.	NIST SP 800-28 Version 2
active cyber defense (ACD)	Synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities.	DSOC
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.	OMB Circular A-130, Appendix III
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.	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.	FIPS 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 that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.	NIST SP 800-39
adversary	Person, group, organization, or government that conducts or has the intent to conduct detrimental activities.	NIST SP 800-30 Rev. 1 (adapted); DHS Lexicon
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.	44 U.S.C. Sec. 3502
	See also *executive agency*.	

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).	IETF RFC 4949 Ver 2
alert	A brief, usually human-readable, technical notification regarding current vulnerabilities, exploits, and other security issues. Also known as an advisory, bulletin, or vulnerability note.	NIST SP 800-150
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 https://www.state.gov.	CNSSI No. 4005
allocation	The process an organization employs to assign security or privacy requirements to an information system or its environment of operation; or to assign controls to specific system elements responsible for providing a security or privacy capability (e.g., router, server, remote sensor).	NIST SP 800-37 Rev. 2
	The process an organization employs to determine whether security controls are defined as system-specific, hybrid, or common.	
all-source intelligence	In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked.	DoD JP 2-0
	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.	NIST SP 800-53 Rev. 5 (adapted)

	Note: Intelligence is limited to the products, activities, and organizations within the Intelligence Community. Related products, activities, and organizations outside of the Intelligence Community are called "information" or "data".	
	See *intelligence.*	
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.	CNSSI No. 4005
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.	NIST SP 800-30 Rev. 1
anti-jam	The result of measures to resist attempts to interfere with communications reception.	CNSSI No. 1200
anti-signal fingerprint	Result of measures used to resist attempts to uniquely identify a particular transmitter based on its signal parameters.	CNSSI No. 1200
anti-signal spoof	Result of measures used to resist attempts to achieve imitative or manipulative communications deception based on signal parameters.	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 prevent physical manipulation or delay exploitation of critical program information in U.S. defense systems in domestic and export configurations to impede countermeasure development, unintended technology transfer, or alteration of a system due to reverse engineering.	DoDI 5200.39 (adapted)
	See *tampering*.	
application	A software program hosted by an information system.	NIST SP 800-37 Rev. 2
application-specific integrated circuits (ASICs) (C.F.D.)	A digital or analog circuit, custom-designed and/or custom-manufactured to perform a specific function. An ASIC is not reconfigurable and cannot contain additional instructions.	Encyclopedia Britannica (adapted)
	C.F.D. Rationale: term is outdated and not regularly used.	
approval to operate (ATO)	See *authorization to operate.*	
approved cryptography	Federal Information Processing Standard (FIPS)-approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation.	NIST SP 800-63-3

artificial intelligence	(1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets. (2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. (3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks. (4) A set of techniques, including machine learning, that is designed to approximate a cognitive task. (5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.	Public Law 115-232, Sec. 238
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.	DoDM 4140.01, Volume 2
assertion	A statement from a verifier to a Relying Party (RP) that contains information about a subscriber. Assertions also may contain verified attributes.	NIST SP 800-63-3
assessment activities [information system context]	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).	NIST SP 800-53A Rev. 4 (adapted)
assessment approach [risk]	The approach used to assess risk and its contributing risk factors, including quantitatively, qualitatively, or semi-quantitatively.	NIST SP 800-30 Rev. 1

assessment findings	Assessment results produced by the application of an assessment procedure to a security control, privacy 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.	NIST SP 800-53A Rev. 4
assessment [general context]	An evidence-based evaluation and judgement on the nature, characteristics, quality, effectiveness, intent, impact, or capabilities of an item, organization, group, policy, activity, or person.	
	Note: Assessments are generally informational in nature and used to support decision making and to inform formal inspections or audits. Assessments may consider information garnered from past audits, inspections, risk analyses, incident reports, intelligence collection, and other related activities, but are considered separate from these activities.	
	See also *threat assessment*, *risk assessment*, *assessment (security control)*. Contrast with *inspection*, *audit (general).*	
assessment method	One of three types of actions (i.e., examine, interview, test) taken by assessors in obtaining evidence during an assessment.	NIST SP 800-53A Rev. 4
assessment object	The item (i.e., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.	NIST SP 800-53A Rev. 4
assessment objective	A set of determination statements that expresses the desired outcome for the assessment of a security control, privacy control, or control enhancement.	NIST SP 800-53A Rev. 4
assessment procedure	A set of assessment objectives and an associated set of assessment methods and assessment objects.	NIST SP 800-53A Rev. 4
assessment (risk)	See *risk assessment*.	

assessment (security control)	The testing or evaluation of the controls in an information system or an organization 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 or privacy requirements for the system or the organization.	NIST SP 800-37 Rev. 2
assessment (threat)	See *threat assessment*.	
assessor	The individual, group, or organization responsible for conducting a security or privacy assessment. See *control assessor* and *risk assessor*.	NIST SP 800-37 Rev. 2
asset	A distinguishable entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and employed, owned, or operated by domestic, foreign, public, or private sector organizations.	DoDD 3020.40
	An item of value to the achievement of organizational mission/business objectives. Note 1: Assets have interrelated characteristics that include value, criticality, and the degree to which they are relied upon to achieve organizational mission/business objectives. From these characteristics, appropriate protections are to be engineered into solutions employed by the organization. Note 2: An asset may be tangible (e.g., physical item such as hardware, software, firmware, computing platform, network device, or other technology components) or intangible (e.g., information, data, trademark, copyright, patent, intellectual property, image, or reputation).	NIST SP 800-160 Vol. 1 (adapted)
asset reporting format (ARF)	A format for expressing the transport format of information about assets and the relationships between assets and reports.	NIST SP 800-126 Rev. 3

assurance	The grounds for confidence that a [security or privacy] claim has been or will be achieved	NIST SP 800-37 Rev. 2
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.	NIST SP 800-39
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 pipeline (AP)	A set of filter processes that are arranged in a linear order using one-way inter-process communications to transfer data between processes. The linear flow is enforced with mandatory and discretionary access control mechanisms.	
asymmetric cryptography	See *public key cryptography (PKC)*.	
asymmetric key algorithm	Asymmetric key algorithms (often called public key algorithms) use a pair of keys (i.e., a key pair): a public key and a private key that are mathematically related to each other. In asymmetric key cryptography, only one key in the key pair, the private key, must be kept secret; the other key can be made public. Asymmetric key cryptography is commonly used to protect the integrity and authenticity of information and to establish symmetric keys.	NIST SP 800-57 Part 2 Rev. 1
asymmetric keys	Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.	FIPS 201-2
attack	See *cyber attack [national security]*	
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.	NIST SP 800-61 Rev. 2 (adapted)
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.	IETF RFC 4949 Ver 2
attended	Under continuous positive control of personnel authorized for access or use.	CNSSI No. 4005
attribute	A quality or characteristic ascribed to someone or something.	NIST SP 800-63-3
attribute-based access control (ABAC)	An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions.	NIST SP 800-162
attribute bundle	A packaged set of attributes, usually contained within an assertion.	NIST SP 800-63-3 (adapted)
attribute reference	A statement asserting a property of an entity without necessarily containing identity information, independent of format. For example, for the attribute "birthday," a reference could be "older than 18" or "born in December."	NIST SP 800-63-3 (adapted)
attribute service	A service that provides a common access point to accurate and current attributes obtained from one or more authoritative attribute sources.	UIAS v2.1 (adapted)
attribute value	A complete statement asserting a property of an entity, independent of format. For example, for the attribute "birthday," a value could be "12/1/1980" or "December 1, 1980."	NIST SP 800-63-3 (adapted)

audit [general context]	Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. Note 1: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines). Note 2: An internal audit is conducted by the organization itself, or by an external party on its behalf.	ISO 30401:2018
audit (data)	Examination of data for quality and accuracy.	ISO 30400:2016 (adapted)
audit (security)	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.	NIST SP 800-82 Rev 2 (under *Audit and Accountability*)
	Note: In some publications, *audit* is used in conjunction or synonymously with the terms *inspection* or *assessment*; these terms are not interchangeable.	
audit (supplier process)	Review of an organization's capacity to meet, or continue to meet, initial and ongoing requirements as a product or service provider.	ISO 15638-1:2012 (adapted)
	Note: Auditable requirements are set forth in agreements (e.g. contracts) and may include security, privacy, quality, or other requirements.	
audit log	A chronological record of system activities, including records of system accesses and operations performed in a given period.	NIST SP 800-171 Rev 2
	Also called "event log" or "security log". See *audit trail.*	
audit record	An individual entry in an audit log related to an audited event.	NIST SP 800-53 Rev. 5

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. These tools generally remove records generated by specific classes of events, such as records generated by nightly backups.	
audit trail	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result.	**NCSC-TG-004*
	A record showing who has accessed an information technology (IT) system and what operations the user has performed during a given period.	NIST SP 800-47
authenticated protected channel	An encrypted communication channel that uses approved cryptography where the connection initiator (client) has authenticated the recipient (server).	NIST SP 800-63-3 (adapted)
authentication	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.	CNSSI No. 4005
	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.	FIPS 200
authentication mechanism	Hardware or software-based mechanisms that force users to prove their identity before accessing data on a device.	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	A defined sequence of messages between a claimant and a verifier that demonstrates that the claimant has possession and control of one or more valid authenticators to establish their identity, and, optionally, demonstrates that the claimant is communicating with the intended verifier.	NIST SP 800-63-3
authenticator	Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. In previous editions of SP 800-63, this was referred to as a *token*.	NIST SP 800-63-3
	An entity that facilitates authentication of other entities attached to the same LAN using a public key certificate.	
authenticator assurance level (AAL)	A category describing the strength of the authentication process.	NIST SP 800-63-3
	Note: NIST SP 800-63-3 describes three levels of strength.	
authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, message, or message originator. See *authentication*.	NIST SP 800-53 Rev. 5; NIST SP 800-39
authoritative attribute source	The official source that originates and maintains the attributes of entities.	UIAS v2.1
authority [privacy context]	A privacy principle (FIPP) that limits an organization's creation, collection, use, processing, storage, maintaining, disseminating, or disclosing of PII to activities for which they have authority to do so, and identify this authority in appropriate notices.	OMB Circular A-130 (adapted)
authorization	Access privileges granted to a user, program, or process or the act of granting those privileges.	NIST SP 800-63-3 (adapted)
	Formerly known as "accreditation."	

authorization boundary	All components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected.	OMB Circular A-130
	Formerly known as "accreditation boundary".	
authorization package	The essential information that an authorizing official uses to determine whether to authorize the operation of an information system or the provision of a designated set of common controls. At a minimum, the authorization package includes an executive summary, system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.	OMB Circular A-130
	Formerly known as "accreditation package".	
authorization to operate (ATO)	The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.	OMB Circular A-130
	Note 1: The system is authorized to operate for a specified period in accordance with terms and conditions established by the authorizing official. Note 2: Formerly known as "approval to operate." Term was replaced in the risk management framework in 2010.	
authorized ID	The key management entity (KME) authorized to order against a traditional short title.	CNSSI No. 4005

authorized user	Any appropriately cleared individual with a requirement to access an information system (IS) for performing or assisting in a lawful and authorized governmental function.	DoDD 8140.01 (adapted)
authorizing official (AO)	A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.	OMB Circular A-130
	Formerly known as "accrediting official" or "accrediting authority" or "designated accrediting authority".	
authorizing official designated representative (AODR)	An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with the authorization process.	NIST SP 800-37 Rev. 2
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 *continuous monitoring* and *information security continuous monitoring (ISCM).*	
automatic remote rekeying	Procedure to rekey distant cryptographic equipment electronically without specific actions by the receiving terminal operator.	
	See *manual remote rekeying*.	
availability	Ensuring timely and reliable access to and use of information.	44 U.S.C. Sec 3552
backdoor	An undocumented way of gaining access to computer system. A backdoor is a potential security risk.	NIST SP 800-82 Rev. 2
backup	A copy of files and programs made to facilitate recovery, if necessary.	NIST SP 800-34 Rev. 1

banner	Display on an information system that sets parameters for system or data use.	
baseline	A specification or work product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures.	NIST SP 800-160, Volume 1, page 223 footnote
baseline configuration	A documented set of specifications for a 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.	NIST SP 800-171 Rev. 2
basic testing	See *black box testing.*	
bastion host	A special purpose computer on a network 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.	CNSSI No. 1011
benign environment	A non-hostile location protected from external hostile elements by physical, personnel, and procedural security countermeasures.	**NCSC-TG-004 (adapted)*
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).	
Big Data	Extensive datasets—primarily in the characteristics of volume, variety, velocity, and/or variability—that require a scalable architecture for efficient storage, manipulation, and analysis.	NIST SP 1500 Vol 1 Rev. 3
binding	Assurance of the integrity of an asserted relationship between items of information that is provided by cryptographic means.	NIST SP 800-56 B Rev. 2 (adapted)

	Process of mapping, associating, or connecting two related elements (e.g., information, data, systems, system components)	NIST SP 800-32 (adapted)
	An association between a subscriber identity and an authenticator or given subscriber session.	NIST SP 800-63-3
biometric(s)	A measurable, physical characteristic or personal behavioral trait used to identify, or verify the claimed identity of, an individual. Facial images, fingerprints, and iris image samples are all examples of biometrics.	FIPS 201-2 (adapted)
	A physical or behavioral characteristic of a human being.	NIST SP 800-32
	Automated recognition of individuals based on their biological and behavioral characteristics.	NIST SP 800-63-3
	Note: Biometrics may be static or dynamic (e.g., requiring continuous or multiple verifications over time).	
bit	A binary digit having a value of 0 or 1.	FIPS 197
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	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.	CNSSI No. 4005
	Designation applied to information systems, and to associated areas, circuits, components, and equipment, in which national security information is encrypted or is not processed.	CNSSAM TEMPEST/1-13; NSTISSI 7002 (adapted)

black box testing	A method of software testing that examines the functionality of an application without peering into its internal structures of workings. This method of test can be applied to virtually every level of software testing: unit, integration, system, and acceptance.	NIST SP 800-192
	Synonymous with "basic testing". Contrast with *white box testing.*	
black core	See *black transport.*	
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.	CNSSI No. 4005
blacklist	A blacklist is a list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications, that have been previously determined to be associated with malicious activity. Note: Blacklist is also known by the terms "block list/blocklist" and "deny list/denylist." See *dirty word list*. Compare with *graylist* and *whitelist*.	NIST SP 800-167 (adapted)
blacklisting	A process used to identify software programs that are not authorized to execute on a system or prohibited Universal Resource Locators (URL)/websites. Note: Blacklisting is also known by the terms "block listing/blocklisting" and "deny listing/denylisting." Compare with *whitelisting*.	NIST SP 800-171 Rev. 2
black transport	A network environment (point-to-point and multi-point) supporting end-to-end encrypted information at a single classification level; networks within the environment are segmented by network technology with inspection points at the perimeter, boundary, or gateway. Encrypted traffic is routed, switched, or forwarded over an unclassified or untrusted network infrastructure.	DoD JIE NNT IDT WAN SA (adapted)

blended attack	A type of attack that combines multiple attack methods against one or more vulnerabilities.	**NIST SP 800-61 Rev. 1*
	Note: This definition is sometimes referred to as "complex attack" or *complex threat.*	
	Deliberate, aggressive action that causes harm to both cyber and physical systems.	H-ISAC
blended threat	A danger that originates in one domain and has the potential to impact another domain, for example a CS attack that impacts the safety of physical systems.	H-ISAC (adapted)
	Contrast with *complex threat.*	
blue team	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 CS 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.	

	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).	
body of evidence (BoE)	The totality of evidence used to substantiate trust, trustworthiness, and risk relative to the system.	NIST SP 800-160 Volume 1
boundary	Physical or logical perimeter of a system.	
	See *authorization boundary.*	
boundary (functional)	Physical or logical perimeter of a set of interacting elements, typically determined relative to the authorization boundary. However, it can also be determined by other "boundaries" established by programmatic, operational, or jurisdictional control. The system functional boundary provides the basis for the security perspective relative to all interactions and behavior with enabling systems, other systems, and the physical environment.	NIST SP 800-160 (adapted from note under "system of interest", and text on page 96)
boundary protection	Monitoring and control of communications at the external interface to a system to prevent and detect malicious and other unauthorized communications using boundary protection devices.	NIST SP 800-53 Rev. 5
boundary protection device	A device (e.g., gateway, router, firewall, guard, or encrypted tunnel) that facilitates the adjudication of different system security policies for connected systems or private boundary protection. The boundary may be the authorization boundary for a system, the organizational network boundary, or a logical boundary defined by the organization.	NIST SP 800-53 Rev. 5

breach [privacy context]	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses personally identifiable information for an other than authorized purpose.	OMB Memorandum 17-12
bridging	Facilitating interoperation by the act of transforming the syntax and semantics of data and control from one type of access control system to another.	
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 intended capacity allocated (due to insecure or unbound allocation parameters), which overwrites 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.	CNSSI No. 1011 (adapted)
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.	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.	NIST SP 800-34 Rev. 1

	Process of analyzing operational functions and the effect that a disruption might have on them.	ISO/IEC 27031-2011
cascading [cross domain]	An approach for deploying CDS where two identical CDSs are placed in series to transfer information across multiple different security domains. Note: DoDI 8540.01 prohibits cascading.	DoDI 8540.01
categorization	See *security categorization.*	
central audit and logging daemon (CALD)	A process that is responsible for receiving audit and log events from system components, syntactically and semantically filtering the audit/log events, and dispatching to the appropriate processes for storage, remote transfer, performance analysis, and system monitoring and remediation.	
central facility (or Tier 0)	See *Tier 0 (central facility)*.	
central journal daemon (CJD)	A process that is responsible for receiving and securely wrapping the content filtered by the CDS and dispatching it for storage and remote transfer. This daemon is also used to send quarantined data (e.g., data that failed filtering) to an external system for analysis.	
central office of record (COR)	The entity that keeps records of accountable COMSEC material held by COMSEC accounts subject to its oversight.	CNSSI No. 4005
central services node (CSN)	The Key Management Infrastructure core node that provides central security management and data management services.	

certificate	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.	CNSSI No. 1300
	See *cross certificate*, *encryption certificate*, and *identity certificate*.	
certificate management	Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed.	
certificate policy (CP)	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.	CNSSI No. 1300
	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.	NIST SP 800-32
certificate revocation list (CRL)	A list of revoked public key certificates created and digitally signed by a Certificate Authority.	FIPS 201-2

	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.	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.	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).	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.	NIST SP 800-32 (adapted)
certification [general context]	The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness.	FIPS 201-2
certification [information security context]	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	FIPS 200
certification authority (CA)	An entity authorized to create, sign, issue, and revoke public key certificates.	CNSSI No. 1300 (adapted)
certification practice statement (CPS)	The entity in a Public-Key Infrastructure (PKI) that is responsible for issuing public-key certificates and exacting compliance to a PKI policy.	NIST SP 800-56B Rev. 2 (adapted)

	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).	NIST SP 800-32
certification test and evaluation (CT&E)	Software, hardware, and firmware 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.	CNSSAM TEMPEST/1-13
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 any transfers.	NIST SP 800-101 Rev. 1
chaining [cross domain]	An approach for deploying CDS where two different CDS on different operating systems are placed in series to transfer information across multiple security domains.	DoDI 8540.01 (adapted)
	Compare with *cascading*.	

challenge and response	An authentication protocol where the verifier sends the claimant a challenge (usually a random value or nonce) that the claimant combines with a secret (such as by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the verifier. The verifier can independently verify the response generated by the claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the claimant possesses and controls the secret.	NIST SP 800-63-3
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.	IETF RFC 4949 Ver 2
chief information officer (CIO)	Executive agency official responsible for: (1) providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (2) developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency; and (3) promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency.	40 U.S.C. Sec. 11315 (b) (adapted);

	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.	
chief information security officer (CISO)	See *senior agency information security officer (SAISO)*.	
cipher	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.	
	Series of transformations that converts plaintext to ciphertext using the Cipher Key.	FIPS 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*.	NIST SP 800-57 Part 1 Rev. 5
claimant	A subject whose identity is to be verified using one or more authentication protocols.	NIST SP 800-63-3
classified information	Information that Executive Order 13526, "Classified National Security Information," December 29, 2009 (3 CFR, 2010 Comp., p. 298), or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, requires agencies to mark with classified markings and protect against unauthorized disclosure.	32 CFR Vol 6 Part 2002.4
	Note: Synonymous with classified national security information (CNSI) (see E.O. 13526). Often used interchangeably with national security information (NSI) (see E.O. 13526).	
	See *national security information, controlled unclassified information*.	
classified information spillage	See *spillage*.	
classified national security information	See *national security information*.	E.O. 13526

clean word list	List of words that are acceptable, but would normally be rejected because they contain a word on the dirty word list (e.g., secret within secretary).	Cross Domain Solution (CDS) Design and Implementation Requirements - 2018 Raise the Bar (RTB) Baseline Release (adapted)
	See *white list, dirty word list.*	
clear	A method of sanitization by applying logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same interface available to the user; 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).	NIST SP 800-88 Rev. 1
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).	CNSSI No. 4005
clear text	Information that is not encrypted. See *plain text*.	NIST SP 800-82 Rev. 2
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.	CNSSI No. 4005

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.	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.	NIST SP 800-145
coalition partner	A nation in an ad hoc defense arrangement with the United States.	CNSSI No. 4005
code [cryptography]	System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length.	NSTISSI 7002
code [programming/software engineering]	Computer instructions and data definitions expressed in a programming language or in a form output by an assembler, compiler, or other translator.	ISO/IEC 24765:2017 (adapted)

code analysis	The act of reverse-engineering a 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.	CNSSI No. 1011 (adapted)
codebook	Document containing plain text and code equivalents in a systematic arrangement, or a technique of machine encryption using a word substitution technique or algorithm that encrypts data in blocks of a specified length.	
cognizant security officer/authority	An entity charged with responsibility for physical, technical, personnel, and information security affecting that organization. Note: Within an organization, there may be a hierarchy of cognizant security officers/authorities existing at a variety of echelons (e.g., a specific geographical area, a specific military base or activity, etc.) with each cognizant security official/authority having sole jurisdiction within that area or activity.	CNSSI No. 4005
	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.	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.	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 other Special Access Program (SAP) category.	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.	CNSSI No. 4005
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.	
commercial national security algorithm (CNSA) Suite	A specific set of cryptographic algorithms and key strengths that may be used to protect classified and unclassified national security systems. Note: The suite was announced in 2015, replacing the former release of Suite B algorithms.	CNSSP No. 15 (adapted)

commercial national security algorithm (CNSA) compatible	A CS or CS-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 CNSA cryptographic algorithms that are functionally supported by the NSA-approved security protocol(s); and c. Has been evaluated or validated in accordance with CNSSP 11.	CNSSP No. 15 (adapted from term Suite B compatible)
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.	NSA/CSS Policy 3-14
commercial solutions for classified (CSfC)	A COTS end-to-end strategy and process in which two or more COTS products can be combined into a solution to protect classified information.	NSA/CSS Policy 3-14 (adapted)
commodity crypto	See *Crypto as an IT Commodity*.	
commodity service	A system service provided by a commercial service provider to a large and diverse set of consumers. The organization acquiring 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 able to require that the provider implement specific security or privacy controls.	NIST SP 800-53 Rev. 5

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.	DoDI 1000.13 (adapted)
common carrier	A telecommunications company that holds itself out to the public for hire to provide communications transmission services.	NIST SP 800-53 Rev. 5
common configuration enumeration (CCE)	A SCAP specification that provides unique, common identifiers for configuration settings found in a wide variety of hardware and software products.	NIST SP 800-128
common control	A security control that is inherited by one or more organizational information systems.	NIST SP 800-37 Rev. 2
	See *control inheritance*.	
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). Note: Previously known as "security control provider."	NIST SP 800-37 Rev. 2
common criteria (CC)	Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems.	
common fill device (CFD)	A COMSEC item used to transfer or store key in electronic form or to insert key into cryptographic equipment.	CNSSI No. 4005 (adapted)

common platform enumeration (CPE)	A SCAP specification that provides a standard naming convention for operating systems, hardware, and applications for the purpose of providing consistent, easily parsed names that can be shared by multiple parties and solutions to refer to the same specific platform type.	NIST SP 800-128
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. Note: Term is not used in the most recent version of CNSSD No. 507 (July 2020), but may still be known to the CNSS community.	**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).	CNSSI No. 4005
common vulnerabilities and exposures (CVE)	An SCAP specification that provides unique, common names for publicly known information system vulnerabilities.	NIST SP 800-128
	A list of entries—each containing an identification number, a description, and at least one public reference—for publicly known CS vulnerabilities.	MITRE CVE
common vulnerability scoring system (CVSS)	An SCAP specification for communicating the characteristics of vulnerabilities and measuring their relative severity.	NIST SP 800-128
common weakness enumeration (CWE) specification	A community-developed formal list or dictionary of common software weaknesses that can occur in software's architecture, design, code or implementation that can lead to exploitable security vulnerabilities.	MITRE CWE FAQs (adapted)
communications cover	See *cover (TRANSEC)*.	

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 CS 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 and information.	**NCSC-TG-004 (adapted)*
community of interest (COI)	A collaborative group of users (working at the appropriate security level or levels) who exchange information in pursuit of their shared goals, interests, missions, or business processes, and must have a shared vocabulary for the information exchanged. The group exchanges information within and between systems.	
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.	
compensating controls	The security and privacy controls employed in lieu of the controls in the baselines described in NIST Special Publication 800-53B that provide equivalent or comparable protection for a system or organization.	NIST SP 800-53 Rev. 5
competent security official	Any cognizant security authority or person designated by the cognizant security authority.	CNSSI No. 4005

complex threat	Two or more separate attacks aimed at the same general or specific target(s) or objective(s) See *blended threat*.	
component	Smallest selectable set of elements on which requirements may be based.	ISO/IEC 15408-1:2009
comprehensive testing	See *white box testing*.	
compromise [automated information systems]	A judgment, based on the preponderance of the evidence, that a disclosure of information to unauthorized persons or a violation of the security policy for a system in which unauthorized, intentional or unintentional disclosure, modification, destruction, or loss of an object has occurred.	CNSSI No. 4003
compromise [cybersecurity/information security]	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.	NIST SP 800-32
compromise [general/intelligence]	The disclosure of classified data to persons not authorized to receive that data.	
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.	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.	CNSSAM TEMPEST/1-13
computer abuse	Intentional or reckless misuse, alteration, disruption, or destruction of information processing resources.	**NCSC-TG-004 (adapted)*
computer forensics	See *digital forensics*.	
computer network attack (CNA)	See *cyber attack [national security]*.	

computer network defense (CND)	See *cyberspace defense*.	
computer network exploitation (CNE)	See *cyberspace exploitation*.	
computer network operation (CNO)	See *cyberspace operations*.	
computer security (COMPUSEC)	See *cybersecurity*.	
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/or VoIP services.	CNSSI No. 5000 (adapted)
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.	CNSSI No. 4005
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. An audit must include an administrative review of procedures, a 100% sighting of all TOP SECRET keying material marked CRYPTO (both physical and electronic) to include hand receipt holders, and a random sampling of all other applicable material (including other keying material, classified and unclassified COMSEC equipment on hand in the account, and on hand receipt).	
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.	CNSSI No. 4005

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.	
COMSEC assembly	See *COMSEC material*.	
COMSEC boundary	See *COMSEC material*.	
COMSEC chip set	See *COMSEC material*.	
COMSEC control program	See *COMSEC material*.	
COMSEC custodian	See *COMSEC account manager*.	
COMSEC demilitarization	See *demilitarize*.	
COMSEC element	See *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.	NSA NAG 16F
COMSEC end-item	Equipment or combination of components ready for use in a COMSEC application.	
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.	

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.	CNSSI No. 4005
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.	CNSSI No. 4005
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.	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.	CNSSI No. 4005
COMSEC manager	See *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 Commercial National Security Algorithm (CNSA) equipment, etc.	CNSSI No. 4005 (adapted)

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.	CNSSI No. 4005
COMSEC module	See *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.	NSTISSD 600
COMSEC service authority	See *service authority*.	
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.	CNSSI No. 4005
COMSEC training	Teaching of skills relating to COMSEC accounting and the use of COMSEC aids.	
concept of operations (CONOP)	See *security concept of operations*.	
confidential algorithm	Cryptographic algorithm that is not publicly available (e.g. proprietary or classified).	

confidentiality [general context]	Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.	44 U.S.C. Sec 3552
confidentiality [data in transit or at rest]	Prevention of compromise of data to unauthorized entities through techniques such as encryption.	
configuration	A collection of an item's descriptive and governing characteristics, which can be expressed in functional terms - i.e., what performance the item is expected to achieve - and in physical terms - i.e., what the item should look like and consist of when it is built. Represents the requirements, design, and implementation that define a particular version of a system or system component.	Defense Acquisition University Glossary
configuration change [system context]	Configuration change is a part of the Configuration Management (CM) process. Broadly, configuration change control activities are a set of processes and approval stages required to change (modify) a configuration item's attributes from an established, documented baseline and then to re-baseline (through the configuration management process) the modified item.	
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.	**NCSC-TG-004*
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 system components that is designated for configuration management and treated as a single entity in the configuration management process.	NIST SP 800-128 (adapted)

configuration management [general context]	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.	NIST SP 800-128
configuration management [acquisition and/or system context]	A management process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design and operational information throughout its life.	Defense Acquisition University Glossary
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 system.	NIST SP 800-128 (adapted)
consent banner	See *security banner*.	
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.	CNSSI No. 1300
contingency key	Key held for use under specific operational conditions or in support of specific contingency plans.	CNSSI No. 4005
contingency plan	A plan that is maintained for disaster response, backup operations, and post-disaster recovery to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.	NIST SP 800-57 Part 1 Rev. 5
	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.	NIST SP 800-34 Rev. 1
continuous monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. See *automated monitoring* and *information security continuous monitoring*.	NIST SP 800-137 (adapted)
control assessment	The testing or evaluation of security controls 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 an information system or organization.	OMB Circular A-130 (under "security control assessment")
	The testing or evaluation of the controls in an information system or an organization 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 or privacy requirements for the system or the organization.	NIST SP 800-37 Rev. 2
	Note: Previously known as "security control assessment"	
control assessor	The individual, group, or organization responsible for conducting a control assessment. See *assessor* and *risk assessor*.	NIST SP 800-37 Rev. 2
	Note: Previously known as "security control assessor"	

control baseline	The set of controls that are applicable to information or an information system to meet legal, regulatory, or policy requirements, as well as address protection needs for the purpose of managing risk.	NIST SP 800-37 Rev. 2
	The set of minimum security controls defined for a low-impact, moderate- impact, or high-impact information system.	FIPS 200 (under "security control baseline")
	Note: Previously known as "security control baseline"	
control correlation identifier (CCI)	Decomposition of a National Institute of Standards and Technology (NIST) control into a single, actionable, measurable statement.	DoDI 8500.01
control enhancement	Augmentation of a control to build in additional, but related, functionality to the control; increase the strength of the control; or add assurance to the control.	NIST SP 800-37 Rev. 2
	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. and/or 3) add assurance to the control.	NIST SP 800-53A Rev. 4 (under "security control enhancement"
	Note: Previously known as "security control enhancement"	
control inheritance	A situation in which a system or application receives protection from controls (or portions of controls) that are developed, implemented, 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*.	NIST SP 800-37 Rev. 2
	Note: Previously known as "security control inheritance"	

control system	A system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include SCADA, DCS, PLCs and other types of industrial measurement and control systems.	NIST SP 800-82 Rev. 2
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 persons or are under continuous physical or electronic surveillance.	CNSSI No. 7003
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.	NIST SP 800-53 Rev. 5
	Contrast with *controlled environment.*	
controlled environment	Any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect CUI from unauthorized access or disclosure.	32 CFR Vol 6 Part 2002.4
	Contrast with *controlled area.*	
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".	CNSSI No. 4001 (adapted)
controlled cryptographic item (CCI) assembly	See *controlled cryptographic item (CCI) component*.	CNSSI No. 4001

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. A CCI component does not perform the entire COMSEC function, and is dependent upon a host equipment or assembly to complete and operate the COMSEC function. Synonymous with controlled cryptographic item (CCI) assembly. Note: CCI component is a collective term and may refer to a single microcircuit, a module, a module set or assembly, a printed circuit board, or any combination of these items.	CNSSI No. 4001 (adapted)
controlled cryptographic item (CCI) equipment	A telecommunications or information handling equipment that embodies a CCI component and performs the entire COMSEC function without dependence on host equipment to operate.	
controlled interface	A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems.	**NIST SP 800-37 Rev. 1*
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 the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see paragraph (e) of this section) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.	32 CFR Vol 6 Part 2002.4
	Note: The CUI categories and subcategories are listed in the CUI Registry, available at https://www.archives.gov/cui.	
controlled unclassified information (CUI) Executive Agent (EA)	The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees Federal agency actions to comply with the Order [E.O. 13556 or any successor order]. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).	32 CFR Vol 6 part 2002.4 and 2002.6

controlled unclassified information (CUI) registry	The online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI EA other than this part. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.	32 CFR Vol 6 part 2002.4
	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. The CUI Registry is available at https://www.archives.gov/cui.	
controlling authority (CONAUTH)	The official responsible for directing the operation of a cryptonet and for managing the operational use and control of keying material assigned to the cryptonet.	CNSSI No. 4006
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.	NIST SP 800-28 Version 2

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	See *manual remote rekeying*.	
correctness proof	Formal technique used to prove mathematically that a computer program satisfies its specified requirements	ISO/IEC 24765:2017 (under "proof of correctness")
counterintelligence	Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.	E.O. 12333, as amended
countermeasure	Any action, device, procedure, technique, or other measure that reduces the vulnerability of or threat to a system.	**NCSC-TG-004*
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.	CNSSI No. 4005 (adapted)
course of action (COA) (risk response)	A time-phased or situation-dependent combination of risk response measures.	NIST SP 800-39
cover (TRANSEC)	Result of measures used to obfuscate message externals to resist traffic analysis.	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.	NIST SP 800-53A Rev. 4

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.	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.	
	Analysis of the ability of an insider to exfiltrate data based on the design of a security device.	
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*.	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.	IETF RFC 4949 Ver 2
credential	An object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber.	NIST SP 800-63-3 (adapted)
credential [PIV card context]	Evidence attesting to one's right to credit or authority; in this Standard, it is the PIV Card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual.	FIPS 201-2

credential service provider (CSP)	A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or issue credentials for its own use.	NIST SP 800-63-3
critical	The designation assigned to a capability, system, or asset that without which will significantly degrade or prevent execution of a supported strategic mission.	DoDI 3020.45
critical asset	An asset of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of an organization to fulfill its missions.	DoDD 3020.40 (adapted from the term DCA)
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.	DoDI 5200.44
	A system element that, if compromised, damaged, or failed, could cause a mission or business failure.	NIST SP 800-161
critical infrastructure	System and assets, whether physical or virtual, so vital to the United States 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.	NIST SP 800-30 Rev. 1
critical infrastructure sectors	The 16 sectors designated by PPD-21 as vital to the United States, namely: chemical; commercial facilities; communications; critical manufacturing; dams; the defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.	PPD-21 (adapted)

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.	ISO/IEC 19790:2012 (adapted)
criticality	A measure of the degree to which an organization depends on the asset for the success of a mission or of a business function.	NIST SP 800-60 Vol 1 Rev. 1
	See *criticality level*.	
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).	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.	
	See *criticality*.	
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.	CNSSI No. 1300
	Note: This is a more narrow definition than described in ITU X.509.	
cross domain	The act of manually and/or automatically accessing and/or transferring information between different security domains.	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 dataflow	The combination of a transport protocol, data format(s), direction(s) of the data transfer, source and destination(s) security domains, endpoints providing/receiving the data, and the filtering policy for a specific CDS customer (e.g., human user of the CDS, machine-to-machine connections).	
cross domain dataflow filtering process	A policy that describes the transport protocol, allowed content types, and the content filtering actions required to address the data attack, data hiding and data disclosure risks of the content being transferred. It may also include other restrictions such as file size or allowed security markings and rules on determining how to route the data to the appropriate destination security domain(s) based on the filtering rules applied. The dataflow filtering policy also implements the CDS portion of foreign partner information exchange agreements when a transfer CDS is used to transfer data to a foreign partner.	
cross domain dataflow identifier (dataflow ID)	A unique alphanumeric sequence (usually a universally unique identifier (UUID)) that indicates a specific dataflow. A user (human or machine) of the CDS will be assigned one or more dataflows using dataflow IDs.	
cross domain filter	A process or set of processes that applies cross domain dataflow filtering policy to content. Filters normally implement the concept of least privilege and generally only work on a specific data type (e.g., a PDF filter would process PDF files but not images). Filters can operate on a Pass/Fail model or Pass with Change model.	

cross domain router	The CDS filter process responsible for the transfer of data between assured pipelines/filter orchestration engines operating at different security levels within the CDS. It is sometimes referred to as the Trusted Executive/Subject or Regrader. The cross domain router takes filtered data from the outbound pipeline and sends it to the inbound pipeline.	
cross domain service	An IT service that provides that provides access or transfer of information solutions between different security domains.	DoDI 8540.01
cross domain solution (CDS)	A form of controlled interface that provides the ability to manually and/or automatically access and transfer information between different security domains. A CDS may consist of one or more devices.	CNSSI No. 1253F Attachment 3 (adapted)
cross domain solution (CDS) baseline list	A list managed by the National Cross Domain Strategy and Management Office (NCDSMO) that identifies CDSs that have been tested by the NCDSMO and are available for deployment within the United States Government.	DoDI 8540.01(adapted)
cross domain solution (CDS) filtering	The process of inspecting data as it traverses a cross domain solution and determining if the data meets pre-defined policy.	DoDI 8540.01
cross domain solution (CDS) process	A software program written or integrated by a CDS developer to perform a specific set of functions on a CDS. Examples include protocol adapters (e.g. Secure File Transfer Protocol daemon (SFTPd), Hypertext Transfer Protocol daemon (HTTPd)), filters, a filter orchestration engine (FOE), the CALD/CJD, and system or CDS administrative interfaces built specifically for the CDS.	

cross domain solution (CDS) sunset list	A list managed by the National Cross Domain Strategy and Management Office (NCDSMO) 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.	DoDI 8540.01 (adapted)
cross domain transfer	The act of manually or automatically accessing or transferring information between different security domains.	
cross-certificate	A certificate issued from a certification authority (CA) that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two CAs.	CNSSI No. 1300
	A certificate used to establish a trust relationship between two certification authorities.	NIST SP 800-32
cryptanalysis	1. Operations performed to defeat 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 information-system security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or in the algorithm itself.	NIST SP 800-57 Part 1 Rev. 5
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.	CNSSI No. 4005

Crypto as IT (CIT)	Set of high assurance, government cryptographic services, hardware, and software that is accounted for, handled, tested, deployed, updated and refreshed similarly to other commercial IT assets in the USG inventory while maintaining proper positive controls and stringent security standards.	
cryptographic	Pertaining to, or concerned with, cryptography.	
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)	A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output.	NIST SP 800-57 Part 1 Rev. 5
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.	
cryptographic authenticator	An authenticator where the secret is a cryptographic key.	NIST SP 800-63-3
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.	ISO/IEC 19790 :2012
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.	

cryptographic equipment (cryptoequipment)	Equipment that embodies a cryptographic logic.	
cryptographic erase	A method of sanitization in which the Media Encryption Key (MEK) for the encrypted Target Data (or the Key Encryption Key—KEK) is sanitized, making recovery of the decrypted Target Data infeasible.	NIST SP 800-88 Rev. 1
cryptographic high value product (CHVP)	NSA-approved products incorporating only UNCLASSIFIED components and UNCLASSIFIED cryptographic algorithms. This includes COTS products approved by NSA, but does not include Commercial Solutions for Classified (CSfC) or their components, unless an individual component has been approved as a CHVP. Unkeyed CHVPs are not classified or designated as Controlled Cryptographic Items (CCI).	CNSSI No. 4031 (adapted)
cryptographic ignition key (CIK)	A device or electronic key used to unlock the secure mode of cryptographic equipment.	CNSSI No. 4005
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.	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 key	A parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce, reverse, or verify the operation while an entity without knowledge of the key cannot.	NIST SP 800-57 Part 1 Rev. 5
cryptographic key management system (CKMS)	Policies, procedures, devices, and components designed to protect, manage, and distribute cryptographic keys and metadata. A CKMS performs cryptographic key management functions on behalf of one or more entities.	NIST SP 800-130

cryptographic logic	A comprehensive and precisely defined sequence of steps or procedural rules used to produce cipher text from plain text and vice versa.	CNSSI No. 4005 (adapted)
	The embodiment of one (or more) cryptographic algorithm(s) along with alarms, checks, and other processes essential to effective and secure performance of the cryptographic process(es).	
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.	
cryptographic modernization 2 (CM2)	A phase of the broader DoD cryptographic modernization initiative started in 2016 to define and implement the next set of mitigations and improvements to modernize the NSA-certified cryptographic product inventory.	
cryptographic modernization initiative (CMI)	A DoD initiative to modernize the NSA-certified cryptographic product inventory. Also referred to as cryptographic modernization (CM) or CryptoMod.	
cryptographic module	A set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation).	NIST SP 800-63-3
cryptographic net (cryptonet)	Stations that hold a common key. This may include multiple communications networks.	CNSSI No. 4006
cryptographic period (cryptoperiod)	Time span during which each key setting remains in effect.	CNSSI No. 4006

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)	The security or protection resulting from the proper use of technically sound cryptosystems.	**NCSC-TG-004 (under cryptosecurity)*
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.	CNSSI No. 4005
cryptographic synchronization	Process by which a receiving decrypting cryptographic logic attains the same internal state as the transmitting encrypting logic.	
cryptographic system (cryptosystem)	Associated CS items interacting to provide a single means of encryption or decryption. Note: A cryptosystem can be keyed COMSEC equipment, a code, or an authenticator.	CNSSI No. 4006 (adapted)
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.	
cryptography	Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.	
	The science of information hiding and verification. It includes the protocols, algorithms and methodologies to securely and consistently prevent unauthorized access to sensitive information and enable verifiability of the information. The main goals include confidentiality, integrity authentication and source authentication	NIST SP 800-175A
cryptologic	Of or pertaining to cryptology.	NIST SP 800-60 Vol. 1 Rev. 1
cryptology	The mathematical science that deals with cryptanalysis and cryptography.	
	The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence.	NIST SP 800-60 Vol. 1 Rev. 1
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.	CNSSI No. 4006
cyber attack [national security]	Actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires.	DoD JP 3-12 under "cyberspace attack"
	See *attack*.	

cyber effect	The manipulation, disruption, denial, degradation, or destruction of information systems, networks, or physical or virtual infrastructure control by information systems, or information resident thereon.	NSPM-13 (adapted)
cyber incident	See *incident, security-relevant event, event*.	
cyber 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 CS incidents. Also called a "Computer Incident Response Team," "Computer Security Incident Response Team (CSIRT)," or a "CIRC (Computer Incident Response Center or a Computer Incident Response Capability)".	
cybersecurity-enabled information technology product	A product or technology whose primary role is not security, but that provides security services as an associated feature of its intended operating capabilities. To meet the intent of Committee on National Security Systems Policy (CNSSP) 11, acquired CS-enabled products must be evaluated if the CS features are going to be used to perform one of the security services (availability, integrity, confidentiality, authentication, or nonrepudiation). Note: Examples include such products as security-enabled web browsers and screening and security-enabled messaging systems.	NSA/CSS Policy 3-4 (adapted)
cybersecurity (CS)	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.	NSPD-54/HSPD-23

	Note: The term cybersecurity replaced the term information assurance (IA) in the DoD and most USG policy documents in 2014. The term information assurance, in turn, previously replaced the terms information security and computer security in the same way. However, the terms information security and computer security are still used in the USG and elsewhere depending on scope and intent.	
cybersecurity 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.	
cybersecurity component	An application (hardware and/or software) that provides one or more CS capabilities in support of the overall security and operational objectives of a system.	
cybersecurity infrastructure	The underlying security framework that lies beyond an enterprise's defined boundary, but supports its CS and CS-enabled products, its security posture and its risk management plan.	
cybersecurity IT product	Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, nonrepudiation of data), correct known vulnerabilities, or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Note: Examples include such products as data/network encryptors, firewalls, and intrusion detection devices.	
cyberspace	The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computers, information systems, industrial control systems, networks, and embedded processors and controllers. See also *maritime cyberspace*.	NSPM-13

	Often shortened to "cyber"	
cyberspace capability	A device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace.	DoD JP 3-12
cyberspace defense	Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration.	DoD JP 3-12
cyberspace exploitation	Actions taken in cyberspace to gain intelligence, maneuver, collect information, or perform other enabling actions required to prepare for future military operations.	DoD JP 3-12
cyberspace incident	See *incident*. See also *event*, *security-relevant event*, and *intrusion*.	
cyberspace operations (CO)	The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.	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.	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.	IETF RFC 4949 Ver 2
data	Information in a specific representation, usually as a sequence of symbols that have meaning.	IETF RFC 4949 Ver 2
data action [privacy context]	A data life cycle operation, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal.	NIST Privacy Framework, V1.0

data aggregation	Compilation of data that together may provide a holistic view of the data, but may also result in increased risk. The totality of the aggregated data may, for example, be classified, classified at a higher level, result in de-anonymization of entities, disclosure of sensitive (CUI) data, or benefit an adversary. The data may originate from a single source or a variety of multiple source.	
	Contrast with *data compilation*	
data asset	An information-based resource.	
	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., https://www.weather.com) would be a data asset.	
data attack risk	The risk of a file type's or protocol's content being used to exploit a system based on processing (i.e., parsing) that content.	
data compilation	The act of performing operations (e.g. statistical analysis) on a collection of data to derive information from that data. This process may result in increased risk. The summarized or analyzed collection of data may, for example, be classified, classified at a higher level, or benefit an adversary. The data may originate from a single source or a variety of multiple sources.	

data disclosure risk	The risk of a file type's or protocol's potential release of sensitive, perhaps classified, information within the content of a file or protocol due to the complexity inherent within a file type or protocol, as well as a general inability to determine whether or not the content in question should be shared.	
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.	NIST SP 800-47
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.	NSA/CSS Policy 11-1
data hiding risk	The risk of a file type's or protocol's potential to conceal information within its syntactic structure or features. Generally, data hiding risks are more prevalent in file types than in protocols due to the increased complexity of file types and the difficulty in reliably parsing those file types (e.g., inability to precisely decode all the structures in the file).	
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.	**NIST SP 800-33*
data loss	The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.	NIST SP 800-137

data loss prevention	A system's 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.	CNSSI No. 1011
data management	The development, execution, and supervision of plans, policies, programs, and practices that deliver, control, protect, and enhance the value of data and information assets throughout their lifecycles.	DAMA-DMBOK2
data mining	An analytical process that attempts to find correlations or patterns in large data sets for the purpose of data or knowledge discovery.	NIST SP 800-53 Rev. 5
data origin authentication	The corroboration that the source of data received is as claimed.	IETF RFC 4949 Ver 2
	See also *non-repudiation* and *peer entity authentication service.*	
data processing [privacy context]	The collective set of data actions—that is, the complete data life cycle, including, but not limited to: collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal.	NIST Privacy Framework, V1.0 (adapted)
data processing ecosystem [privacy context]	The complex and interconnected relationships among entities involved in creating or deploying systems, products, or services or any components that process data.	NIST Privacy Framework, V1.0
data provenance	See *provenance.*	
data spillage	See *spillage*.	

data steward	A designated group or individual assigned to prepare data collection plans, collect and store program performance data, and analyze and report data in response to performance information requests.	NSA/CSS Policy 1-50
	Data stewards enforce policies, and functional data managers implement the policies and manage day-to-day quality. Data stewards regularly assess classification criteria and test compliance to prevent security issues resulting from data aggregation.	
	Data stewards are legally accountable across the data lifecycle on behalf of the originating element for: a) establishing protection, sharing and governance guidelines for data and datasets within an assigned subject area; b) maintaining data names, business definitions, data integrity rules, and domain values within an assigned subject area; c) compliance with legal and policy requirements and conformance to internal and IC data policies and data standards; d) ensuring application of appropriate security controls; e) analyzing and improving data quality; and f) identifying and resolving related issues.	Intelligence Community (IC) Data Management Lexicon (DML)
	See also *information steward*	
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.	Information Sharing Architecture (ISA) Shared Situational Awareness (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.	
data transfer solution	Interconnected networks or information systems that operate in different security domains and transfer data between them.	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.	IETF RFC 4949 Ver 2
decrypt	A generic term encompassing decoding and deciphering.	
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	An information security strategy that integrates people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.	NIST SP 800-53 Rev. 5
defense industrial base (DIB)	The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development and design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. Also called DIB.	DoD JP 3-27
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.	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.	DoD JP 3-12
degauss	To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Degaussing any current generation hard disk (including but not limited to IDE, EIDE, ATA, SCSI, and Jaz) will render the drive permanently unusable since these drives store track location information on the hard drive.	NIST SP 800-88 Rev. 1
	Also called "demagnetizing."	
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.	NIST SP 800-72
demilitarize	The act of eliminating the functional capabilities and/or inherent military design features [from DoD personal property]. Methods and degree range from removal and destruction of critical features to total destruction by cutting, crushing, shredding, melting, burning, etc. Note: Demilitarization is required to prevent property from being used for its originally intended purpose and to prevent the release of inherent design information that could be used against the United States. Demilitarization applies to material in both serviceable and unserviceable condition.	DoD Manual 4160.28, Volume 1 (adapted)
	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.	CNSSI No. 4004.1 (adapted)
	Note: This term is also known as "DEMIL," and "demilitarization."	

demilitarized zone (DMZ)	A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet.	NIST SP 800-45 Ver 2
	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.	NIST SP 800-41 Rev. 1
	Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's CS 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.	
Department of Defense information network operations	Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve CS on the Department of Defense information networks.	DoD JP 3-12 (adapted)
Department of Defense information networks (DODIN)	The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.	DoD JP 6-0
depth	An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method.	NIST SP 800-53A Rev. 4
derived credential	A credential issued based on proof of possession and control of an authenticator associated with a previously issued credential, so as not to duplicate the identity proofing process.	NIST SP 800-63-3

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.	NIST SP 800-88 Rev. 1
deterministic random bit generator (DRBG)	A random bit generator that includes a DRBG algorithm and (at least initially) has access to a source of randomness. The DRGB produces a sequence of bits from a secret initial value called a seed. A cryptographic DRBG has the additional property that the output is unpredictable given that the seed is not known. A DRBG is sometimes also called a pseudo-random number generator (PRNG) or a deterministic random number generator.	NIST SP 800-57 Part 1 Rev. 5
developer	A general term that includes developers or manufacturers of systems, system components, or system services; systems integrators; vendors; and product resellers. The development of systems, components, or services can occur internally within organizations or through external entities.	NIST SP 800-53 Rev. 5
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 authentication	The process of establishing confidence in user identities presented digitally to a system. In previous editions of SP 800-63, this was referred to as "electronic authentication" or "e-authentication."	NIST SP 800-63-3

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.	DoDD 5505.13E
digital identity	The unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known.	NIST SP 800-63-3
	Note: There is no single, widely accepted definition for this term and context is important. This definition is specific to online transactions.	
digital media	A form of electronic media where data are stored in digital (as opposed to analog) form.	NIST SP 800-53 Rev. 5
digital signature	The result of a cryptographic transformation of data that, when properly implemented with a supporting infrastructure and policy, provides the services of: 1. Source/identity authentication, 2. Data integrity authentication, and/or 3. Support for signer non-repudiation.	NIST SP 800-57 Part 1 Rev. 5
	See also *electronic signature*	

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.	CNSSAM TEMPEST/1-13
directory service (D/S)	Repository of account registration.	CNSSI No. 4005
dirty word list	Words or phrases that are not allowed to appear in given content and are an indication the content is likely not releasable to the destination domain. To be contrasted with clean words, those words that contain a dirty word but are allowed to appear in given content (e.g. if "secret" was a dirty word, then "secretary" could be a clean word).	Cross Domain Solution (CDS) Design and Implementation Requirements - 2018 Raise the Bar (RTB) Baseline Release (adapted)
disaster recovery plan (DRP)	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*.	
	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.	NIST SP 800-34 Rev. 1

discretionary access control	An access control policy that is enforced over all subjects and objects in a system where the policy specifies that a subject that has been granted access to information can do one or more of the following: pass the information to other subjects or objects; grant its privileges to other subjects; change the security attributes of subjects, objects, systems, or system components; choose the security attributes to be associated with newly-created or revised objects; or change the rules governing access control. Mandatory access controls restrict this capability.	NIST SP 800-53 Rev. 5
disposition	The process of reusing, recycling, converting, redistributing, transferring, donating, selling, demilitarizing, treating, destroying, or fulfilling other end of life tasks or actions [for DoD property]. Does not include real (real estate) property.	DoD Manual 4160.21, Volume 1
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).	NIST SP 800-34 Rev. 1 (adapted)
	Incident, whether anticipated (e.g. hurricane) or unanticipated (e.g. power failure/outage, earthquake, or cyber attack) which disrupts an organization's normal course of operations.	ISO/IEC 27031-2011 (adapted)
disassociability	Enabling the processing of information or events without association to individuals or devices beyond the operational requirements of the system.	NISTIR 8062 (adapted)
disassociability [privacy context]	Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system. See also *manageability [privacy context]* and *predictability [privacy context]*.	NISTIR 8062

distinguished name (DN)	An identifier that uniquely represents an object in the X.500 directory information tree.	IETF RFC 4949 Ver 2
distinguishing identifier	See *unique identifier*.	
distributed denial of service (DDoS)	See *active 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.	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*.	NIST SP 800-53 Rev. 5
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.	**NIST SP 800-37 Rev. 1*
effective period	Time span during which each COMSEC key edition (i.e., multiple key segments) remains in effect.	CNSSI No. 4006 (adapted)
electronic authentication (e-authentication)	See *digital authentication*	
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.	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.	CNSSI No. 4005
	Note: EKMS system functionality has been incorporated into key management infrastructure (KMI) 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	A method of signing an electronic message that— (A) identifies and authenticates a particular person as the source of the electronic message; and (B) indicates such person's approval of the information contained in the electronic message.	Public Law 105-277, Sec. 1710
	See also *electronic credentials* and *digital signature*	
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 crypto-equipment and telecommunications systems. See *TEMPEST*.	DoD JP 6-0

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.	ICS 700-1
encipher (C.F.D.)	See *encrypt*.	
	C.F.D Rationale: Deprecated Term; *encrypt* is the preferred term.	
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.	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.	IETF RFC 4949 Ver 2
encrypt	Cryptographically transform data to produce cipher text.	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.	CNSSI No. 4005
encryption	The cryptographic transformation of data to produce ciphertext.	ISO/IEC 7498-2:1989
encryption algorithm	Process which transforms plaintext into ciphertext.	ISO/IEC 18033-1:2021
	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.	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.	
end-to-end encryption	Communications encryption in which data is encrypted when being passed through a network, but routing information remains visible.	NIST SP 800-12, Rev. 1
end-to-end security	Safeguarding information in an information system from point of origin to point of destination.	
enrollment	The process through which an applicant applies to become a subscriber of a credentials service provider (CSP) and the CSP validates the applicant's identity.	NIST SP 800-63-3
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. See *organization*.	
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.	CNSSP No. 24
enterprise audit [general context]	The identification, collection, correlation, analysis, storage and reporting of audit information.	CNSSI 1015 (adapted)
enterprise cross domain services (ECDS)	A set of cross domain services implemented by a government agency or an authorized commercial provider that is able to support a wide set of mission customers, provision new data flows via an established and timely process, and meet enterprise-level scalability and availability requirements, including support for connections to multiple security domains.	CJCSI 6211.02D (adapted)
enterprise cross domain service provider (ECDSP)	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.	DoDI 8540.01

enterprise-hosted cross domain solution (CDS)	A cross domain solution (CDS) that is managed by an enterprise cross domain service provider (ECDSP), but provides cross domain service to a dedicated customer. Enterprise-hosted CDS are frequently former point-to-point CDSs that have been moved from a customer site to an ECDSP.	DoDI 8540.01 (adapted)
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.	
entity	An individual (person), organization, device or process. Used interchangeably with "party".	NIST SP 800-89
entropy	A measure of the amount of uncertainty an attacker faces to determine the value of a secret. Entropy is usually stated in bits. A value having n bits of entropy has the same degree of uncertainty as a uniformly distributed n-bit random value.	NIST SP 800-63-3
environment conditions	Dynamic factors, independent of subject and object, that may be used as attributes at decision time to influence an access decision. Examples of environment conditions include time, location, threat level, and temperature.	NIST SP 800-162

environment of operation	The physical surroundings in which an information system processes, stores, and transmits information.	OMB Circular A-130
	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.	NIST SP 800-30 Rev. 1
erasure	Process intended to render magnetically stored information irretrievable by normal means.	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.	NIST SP 800-152
ethernet data encryption cryptographic interoperability specification (EDE-CIS)	A standard defining the requirements for Ethernet encryption, similar to HAIPE but for layer 2 Ethernet devices.	
evaluating authority	The official responsible for evaluating a reported COMSEC incident for the possibility of compromise.	CNSSI No. 4006
event	Any observable occurrence in a network or system.	NIST SP 800-61 Rev. 2
	See also *cybersecurity event*, *security-relevant event*.	

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.	NIST SP 800-53A Rev. 4
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.	41 U.S.C. Sec. 133
exfiltration	The unauthorized transfer of information from a system.	NIST SP 800-53 Rev. 5
expected output	Any data collected from monitoring and assessments as part of the information security continuous monitoring (ISCM) strategy.	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*.	**NCSC-TG-004 (adapted)*
extensible configuration checklist description format (XCCDF)	A language for authoring security checklists/benchmarks and for reporting results of evaluating them.	NIST SP 800-126 Rev. 3
external system (or component)	A system or system element 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 controls or the assessment of control effectiveness.	NIST SP 800-37 Rev. 2

external system service	A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required controls or the assessment of control effectiveness.	NIST SP 800-37 Rev. 2
External system service provider	A provider of external 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.	NIST SP 800-37 Rev. 2
external network	A network not controlled by the organization.	NIST SP 800-53 Rev. 5
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.	CNSSI No. 4005
extranet	A computer network that an organization uses for application data traffic between the organization and its business partners.	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).	IETF RFC 4949 Ver 2
	Compare with *fail secure* and *fail soft.*	
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).	IETF RFC 4949 Ver 2
	Compare with *fail safe* and *fail soft.*	

fail soft	Selective termination of affected, non-essential system functions when a failure occurs or is detected in the system. Compare with *fail safe* and *fail secure.*	IETF RFC 4949 Ver 2
failover	The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby system upon the failure or abnormal termination of the previously active system.	NIST SP 800-53 Rev. 5
failure access	Type of incident in which unauthorized access to data results from hardware or software failure.	**NCSC-TG-004 (adapted)*
failure control	Methodology used to detect imminent hardware or software failure and provide fail safe or fail soft recovery.	**NCSC-TG-004 (adapted)*
false acceptance	When a biometric system incorrectly identifies an individual or incorrectly authenticates an impostor against a claimed identity.	NIAP Technical Decision 0301 (adapted)
false accept rate (FAR)	Proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed.	ISO/IEC 19795-6:2012
false rejection	When a biometric system fails to identify an enrollee or fails to verify the legitimate claimed identity of an enrollee.	NIAP Technical Decision 0301 (adapted)
false reject rate (FRR)	Proportion of verification transactions with truthful claims of identity that are incorrectly denied.	ISO/IEC 19795-6:2012
fault-tolerance	The ability of a system to continue to run when one or more component(s) of the system fails.	NIST SP 1500 Vol 1 Rev 3 (adapted)

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.	NIST SP 800-30 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.	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.	CNSSP No. 24
federal information processing standards (FIPS)	A standard for adoption and use by Federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology to achieve a common level of quality or some level of interoperability.	FIPS 201-2

federal information processing standards (FIPS)-validated cryptography	A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-3 (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*.	NIST SP 800-53 Rev. 5
federal information security modernization act (FISMA) of 2014	44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283; FISMA directs federal agencies to develop, document, and implement agency-wide programs to provide security for the information and systems that support the agency's operations and assets. This includes the security authorization and accreditation (SA&A) of IT systems that support digital authentication.	NIST SP 800-63-3 (adapted)
	Note: The Federal Information Security Modernization Act replaced the Federal Information Security Management Act of 2002 (44 U.S.C. § 3541) which was enacted by Title 3 of the E-Government Act of 2002 (P.L. 107-347)	
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.	40 U.S.C. Sec 11331
federation	A process that allows the conveyance of identity and authentication information across a set of networked systems.	NIST SP 800-63-3
federation assurance level (FAL)	A category describing the assertion protocol used by the federation to communicate authentication and attribute information (if applicable) to a relying party (RP).	NIST SP 800-63-3 (adapted)
	Note: NIST SP 800-63-3 describes three levels of assurance.	

federation proxy	A component that acts as a logical RP to a set of IdPs and a logical IdP to a set of RPs, bridging the two systems with a single component. These are sometimes referred to as "brokers."	NIST SP 800-63-3
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.	**NCSC-TG-004 (adapted)*
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.	CNSSI No. 4005
filter artifact	Content that has been extracted so that it can be filtered by other content specific filters (e.g., a JPEG image in an MS Word document would be a filtering artifact once it has been extracted by the MS Word filter for further filtering by the CDS's JPEG filter).	
filter orchestration engine (FOE)	A set of processes used to coordinate the filtering of content being transferred through the CDS. The FOE processes determine which dataflow filtering policy will be used, sends the content to the filter(s) to be processed, notifies the filter(s) which dataflow filtering policy to use, retrieves the content and artifacts from the filters, determines if additional filtering is required and validates that the filtering performed is what was required and the content passed all required filtering.	
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.	CNSSI No. 4005

firewall	A part of a computer system or network that is designed to block unauthorized access while permitting outward communication.	NIST SP 800-152
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. See *hardware* and *software*.	IETF RFC 4949 Ver 2
fixed COMSEC facility	COMSEC facility located in an immobile structure or aboard a ship.	CNSSI No. 4005
fixed format data	A type of data that can be defined and validated via a ruleset or schema. Examples include eXtensible Markup Language (XML), JavaScript Object Notation (JSON), Key-Length-Value (KLV), United States Message Text Format (USMTF), Tactical Digital Information Link-J (TADIL-J), and Variable Message Format (VMF). Fixed format data can be textual or binary. Fixed format data is primarily used for machine-to-machine messaging and is generally designed to be efficiently processed by software.	
flooding	An attack that attempts to cause a failure in a system by providing more input than the system can process properly.	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.	CNSSD No. 504
focused testing	See *gray box testing*	

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.	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.	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.	NIST SP 800-53 Rev. 5 [adapted from SA-17(1)]
free and open source software (FOSS)	Software that is liberally licensed to grant users the right to use, copy, study, change, and improve its design through the availability of its source code. In the context of free and open source software, free refers to the freedom to copy and reuse the software. FOSS is an inclusive term that covers both free software and open source software	NSA/CSS Policy 6-10

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 context]	Complete diagnostic repair, modification, and overhaul of COMSEC equipment down to replacement of piece parts on Printed Wiring Assemblies/Circuit Card Assemblies, as well as replacement of chassis-mounted parts. See *limited maintenance*.	CNSSI No. 4000
functional testing	Segment of quality assurance testing in which advertised security mechanisms of an information system are tested against a specification.	**NCSC-TG-004 (adapted)*
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.	IETF RFC 4949 Ver 2
general purpose enterprise cross domain service (GP-ECDS)	An enterprise cross domain service available to authorized users of connected networks that supports a broad range of data types.	DISN CPG (adapted)
general purpose enterprise cross domain service provider (GP-ECDSP)	An ECDSP providing an enterprise cross domain service that is available to all authorized users of the ECDSP's supported security domains with support for a broad range of data types.	DISN CPG (adapted)
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.	OMB Circular A-130, Appendix III

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.	NSA/CSS Policy 3-14
gray box testing	A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. Also known as focused testing.	
graylist	A list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications, that have not yet been established as benign or malicious; more information is needed to move graylist items onto a whitelist or a blacklist. Compare with *whitelist* and *blacklist*.	NIST SP 800-167 (adapted)
gray market	Distribution channels which, while legal, are unofficial, unauthorized, or unintended by the original manufacturer.	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.	IETF RFC 4949 Ver 2
	See *transfer cross domain solution*.	

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.	CNSSI No. 4005
hand receipt holder	A user to whom COMSEC material has been issued a hand receipt. Known in EKMS and KMI as a Local Element.	CNSSI No. 4005
handshake	Protocol dialogue between two systems for identifying and authenticating themselves to each other, or for synchronizing their operations with each other.	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).	
hardware	The material physical components of an information system. See *firmware* and *software*.	IETF RFC 4949 Ver 2
hash function	A function that maps a bit string of arbitrary (although bounded) length to a fixed-length bit string. Approved hash functions satisfy the following properties: 1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output. 2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.	NIST SP 800-57 Part 1 Rev. 5
	Note: often referred to as "hash algorithm" or "cryptographic hash function"	
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.	FIPS 198-1 (adapted)
hashing	The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.	NIST SP 800-72
hazard	A condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation.	DoD Dictionary (as amended)
high assurance internet protocol encryptor (HAIPE)	Device that provides networking, traffic protection, and management features that provide CS services in an IPv4/IPv6 network.	CNSSP No. 19 (adapted)
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.	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 not able to perform one or more of its primary functions; 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.)	FIPS 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 199 potential impact value of high.	FIPS 200

	Note: For National Security Systems, CNSSI No. 1253 assigns one impact value (low, moderate, or high) for each of the three security objectives (confidentiality, integrity, and availability), rather than using the FIPS 200 high water mark across security objectives.	
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*.	CNSSAM TEMPEST/1-13
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.	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.	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.	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.	NIST SP 800-34 Rev. 1

hunt team	A group of individuals that operate within consenting customer networks and systems to detect, characterize, and enable the eradication of malicious cyber actors that evade detection by other information security methods. Hunt teams may leverage direct access to network devices and administrators, as well as operational security measures, to collect data about network systems, traffic, users, and resources in order to detect malicious cyber actors.	
hybrid control	A security or privacy control that is implemented for a system in part as a common control and in part as a system-specific control. See *common control* and *system-specific security control*.	OMB Circular A-130 (adapted)
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.	FIPS 201-2
identifier	Unique data used to represent a person's identity and associated attributes. A name or a PIV card number are examples of identifiers.	FIPS 201-2 (adapted)
	Note: This also encompasses non-person entities (NPEs).	
identity	An attribute or set of attributes that uniquely describe a subject within a given context.	NIST SP 800-63-3
	The set of physical and behavioral characteristics by which an individual is uniquely recognizable.	FIPS 201-2
	Note: This also encompasses non-person entities (NPEs).	
identity assurance level (IAL)	A category that conveys the degree of confidence that the applicant's claimed identity is their real identity.	NIST SP 800-63-3 (adapted)

	Note: NIST SP 800-63-3 describes three levels of assurance.	
identity-based access control (IBAC)	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.	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.	FICAM Roadmap and Implementation Guidance V2.0
identity proofing	The process by which a credential service provider (CSP) collects, validates, and verifies information about a person. Note: Identity proofing establishes that a subject is actually who they claim to be.	NIST SP 800-63-3
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.	FIPS 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.	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.	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 actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. See also *event*, *security-relevant event*, and *intrusion*.	44 U.S.C. Sec 3552
incident handling	The remediation or mitigation of violations of security policies and recommended practices.	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).	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	A pattern of relevant observable adversary activity in the operational cyber domain. See *precursor*.	
individuals	An assessment object that includes people applying specifications, mechanisms, or activities.	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.	
individual participation [privacy context]	A privacy principle (FIPP) that encourages an organization to involve the individual in the process of using PII and, to the extent practicable, for the organization to seek consent from the individual for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII as well as for the organization to establish procedures to handle privacy-related complaints and inquiries.	OMB Circular A-130 (adapted)
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).	NIST SP 800-82 Rev. 2

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.	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).	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. See *cybersecurity (CS)*.	
	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. An information domain may contain data that is at different security levels, and not all data in an information domain is releasable or discloseable to all participants. Participants in an information domain must acknowledge the increased risk of the potential for unintended release or disclosure of information. Note: Information domains may be authorized to use alternative separation and isolation mechanisms to protect data in lieu of a cross domain solution.	
information environment	The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.	DoD 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.	**NCSC-TG-004 (adapted)*
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."	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 also *information steward*.	FIPS 200
information resources	Information and related resources, such as personnel, equipment, funds, and information technology.	44 U.S.C. Sec 3502
information resources management (IRM)	The process of managing information resources to accomplish agency missions and to improve agency performance, including through the reduction of information collection burdens on the public.	44 U.S.C. Sec 3502
information security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability. See *cybersecurity (CS)*.	44 U.S.C. Sec 3552
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.	NIST SP 800-37 Rev. 2
information security continuous monitoring (ISCM)	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.	NIST SP 800-137

	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 *continuous monitoring* and *automated security monitoring*.	
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.	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.	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.	NIST SP 800-37 Rev 2

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*.	NIST SP 800-30 Rev. 1
information sensitivity level	See *security level*.	
information sharing environment (ISE)	The people, projects, systems, and agencies that enable responsible information sharing across the national security enterprise, sharing that includes information on terrorism, homeland security, and countering weapons of mass destruction.	DNI ISE, About the ISE (adapted)
	Note: ISE in its broader application enables those in a trusted partnership to share, discover, and access controlled information, and it promotes partnerships across federal, state, local, and tribal governments, the private sector, and internationally.	
information steward	An agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.	NIST SP 800-37 Rev. 2
information system (IS)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.	44 U.S.C. Sec 3502
information system boundary	See *authorization boundary*, *boundary*.	
information system component	See *system component*.	
information system lifecycle	See *system life cycle*.	
information system owner (or program manager)	See *system owner*.	

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.	NIST SP 800-39
information system-related privacy risks	Risks that arise from either 1) a breach (privacy context), or 2) as a result of authorized data processing activities that produce a problematic result and reflect the potential adverse impacts to individuals or an organization. Adverse impacts to an organization can include program delays or failures, compliance costs, reputational damage, etc. Adverse impacts to an individual can include the disclosure of private facts, mental pain and emotional distress, potential for blackmail, financial harm, embarrassment, inconvenience, unfairness or unconscious bias, discrimination, loss of trust, etc.	OMB Memorandum 17-12 (adapted); NIST Privacy Framework, V1.0 (adapted); 5 U.S.C., Sec. 552a, Privacy Act of 1974 (adapted)
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*.	NIST SP 800-30 Rev. 1
information system service	See *system service.*	
information systems security (INFOSEC)	See *information assurance (IA).*	
information systems security (INFOSEC) boundary	A definable perimeter encompassing all the critical functions in an INFOSEC product and separating them from all other functions within the product.	IASRD-001-2016 (adapted)
	Contrast with *authorization boundary*. See also *boundary*.	
information systems security engineer (ISSE)	See *systems security engineer*.	

information systems security engineering	See *systems security engineering (SSE).*	
information systems security manager (ISSM)	Individual responsible for the CS of a program, organization, system, or enclave.	OPM Interpretive Guidance for Cybersecurity Positions
information system security officer (ISSO)	See *system security officer (SSO)*	NIST SP 800-37 Rev. 2
	As of 2018, FISMA guidance is moving away from *information system security officer (ISSO)* in favor of the broader term, *system security officer (SSO).*	
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.	40 U.S.C. Sec. 11101 (adapted)
information technology product	See *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.	FIPS 199

information value	A qualitative measure of the importance of the information based upon factors such as the level of robustness of security controls allocated to the protection of information based upon: mission criticality, the sensitivity (e.g., classification and compartmentalization) of the information, releasability or privacy requirements, 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 *control inheritance*.	
initial security control set	The set of security controls resulting from the combination of a baseline and applicable overlays prior to system specific tailoring.	CNSSI No. 1253
insider	Any person with authorized access to any organizational resource, to include personnel, facilities, information, equipment, networks, or systems	NIST SP 800-53 Rev. 5
insider threat	The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of organizational operations and assets, individuals, other organizations, and the Nation. This threat can include damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of organizational resources or capabilities.	NIST SP 800-53 Rev. 5
insider threat program	A coordinated collection of capabilities authorized by the organization and used to deter, detect, and mitigate the unauthorized disclosure of information.	NIST SP 800-53 Rev. 5

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.	CNSSAM TEMPEST/1-13 (adapted)
inspection	Examination of an information system to determine compliance with security policy, procedures, and practices.	
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.	CNSSI No. 4001
	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).	
integrity	Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.	44 U.S.C. Sec. 3552
	Rules that govern the modification and destruction of system elements (including, but not limited to, data and information) and that govern the manner in which system elements can be manipulated.	NIST SP 800-160 Vol 1
	Note: a loss of integrity is the unauthorized modification or destruction of information, as described in FIPS 199.	

intellectual property	Refers broadly to the creations of the human mind. IP rights protect the interests of innovators and creators by giving them rights over their creations. IP is usually divided into two branches, namely industrial property and copyright. Industrial property takes a range of forms, including patents for inventions, industrial designs, trademarks, service marks, layout-designs of integrated circuits, commercial names and designations, geographical indications and protection against unfair competition. Copyright relates to literary and artistic creations, such as books, music, paintings and sculptures, films and technology-based works (such as computer programs and electronic databases). In certain languages, copyright is referred to as authors' rights.	World Intellectual Property Organization (WIPO)
intelligence	Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons.	10 CFR 709.2
	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.	DoD JP 2-0
	Note: Intelligence is limited to the products, activities, and organizations within the Intelligence Community. Related products, activities, and organizations outside of the Intelligence Community are called "information" or "data".	
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.	E.O. 12333, as amended

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.	E.O. 12333, as amended; 50 U.S.C. Sec 3003
intelligence community (IC) intelligence technology enterprise (ITE)	The strategic implementation of the IC information environment to enable greater IC integration, information sharing and safeguarding through a new common IC information technology architecture that substantially reduces costs.	ICS 502-01

interconnection security agreement (ISA)	A security document that specifies the technical and security requirements for establishing, operating, and maintaining the interconnection. It also supports the MOU/A between the organizations. Specifically, the ISA documents the requirements for connecting the IT systems, describes the security controls that will be used to protect the systems and data, contains a topological drawing of the interconnection, and provides a signature line.	NIST SP 800-47
interface	Common boundary between independent systems or modules where interactions take place.	
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.	
	See *authorization to operate.*	
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.	CNSSI No. 1300
internal network	A network where the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors. Cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints provides the same effect (at least regarding confidentiality and integrity). An internal network is typically organization-owned yet may be organization-controlled while not being organization-owned.	NIST SP 800-53 Rev. 5

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).	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.	
inter-process communications (IPC)	An operating system mechanism that allows processes to communicate. Mechanisms include (but are not limited to) Transmission Control Protocol (TCP) sockets, User Datagram Protocol (UDP) sockets, Unix Domain Sockets, System V/Portable Operating System Interface for Unix (POSIX) message queues, named pipes (also called a Unix FIFO), System V/POSIX shared memory, signals, System V/POSIX semaphores, and pipes.	
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.	NIST SP 800-53A Rev. 4
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.	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.	IETF RFC 4949 Ver 2
	Unauthorized access to a Federal Government or critical infrastructure network, information system, or application.	NSPD-54/HSPD-23
	Also known as "cyber intrusion" or "cyberspace intrusion"	
intrusion detection	The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents.	NIST SP 800-94
intrusion detection system (IDS)	Software that automates the intrusion detection process.	NIST SP 800-94
intrusion detection and prevention system (IDPS)	Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.	NIST SP 800-61 Rev. 2
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.	NIST SP 800-94
intrusion prevention system (IPS)	Software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. Also called an "intrusion detection and prevention system."	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.	IETF RFC 4301
IT security awareness and training program (C.F.D.)	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)	
	C.F.D. Rationale: The term is being subsumed by the broader term "security awareness and training program".	
inventory [COMSEC]	(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.	CNSSI No. 4005
jamming	An attack that attempts to interfere with the reception of broadcast communications.	IETF RFC 4949 Ver 2
joint authorization	Authorization involving multiple authorizing officials.	NIST SP 800-37 Rev. 2
key	See *cryptographic key*.	
key administration	See *cryptographic key management system (CKMS).*	
key agreement	A key-establishment procedure where keying material is generated from information contributed by two or more participants so that no party can predetermine the value of the keying material independently of any other party's contribution.	NIST SP 800-57 Part 1 Rev. 5

key distribution	The transport of a key and other keying material from an entity that either owns, generates, or otherwise acquires the key to another entity that is intended to use the key.	NIST SP 800-57 Part 1 Rev. 5
key distribution center (KDC)	COMSEC facility generating and distributing key in electronic form.	
key encryption key (KEK)	A key that encrypts another key [typically traffic encryption keys (TEKs)] for transmission or storage.	
key escrow	The retention of the private component of the key pair associated with a subscriber's encryption certificate to support key recovery.	CNSSI No. 1300
key exchange	Process of exchanging public keys (and other information) in order to establish secure communications.	NIST SP 800-32 (adapted)
	See *key transport*	
keyed hash-based message authentication code (HMAC)	A message authentication code that uses a cryptographic key in conjunction with a hash function.	FIPS 198-1
key management	The activities involving the handling of cryptographic keys and other related key information during the entire lifecycle of the keys, including their generation, storage, establishment, entry and output, use and destruction.	NIST SP 800-57 Part 1 Rev. 5
key management device	Any combination of Federal Cryptographic Key Management System (FCKMS) components that serve a specific purpose (e.g., firewalls, routers, transmission devices, cryptographic modules, and data storage devices).	NIST SP 800-152
key management infrastructure (KMI)	A unified, scalable, interoperable, and trusted infrastructure that provides net-centric key management services to systems that rely on cryptography, serving Department of Defense (DoD) and the broader cryptographic community.	DoD 2016 Major Automated Information System Annual Report, Key Management Infrastructure Increment 2

key pair	A public key and its corresponding private key; a key pair is used with a public-key algorithm.	NIST SP 800-57 Part 1 Rev. 5
key recovery	Mechanisms and processes that allow authorized entities to retrieve or reconstruct keys and other key information from key backups or archives.	NIST SP 800-57 Part 2 Rev. 1
keying material	A cryptographic key and other parameters (e.g., IVs or domain parameters) used with a cryptographic algorithm.	NIST SP 800-57 Part 1 Rev. 5
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.	NIST SP 800-12, Rev. 1
key transport	A key-establishment procedure whereby one party (the sender) selects and encrypts (or wraps) the keying material and then distributes it to another party (the receiver). When used in conjunction with a public-key (asymmetric) algorithm, the key is encrypted using the public key of the receiver and subsequently decrypted using receiver's private key. When used in conjunction with a symmetric algorithm, the key is encrypted with a key-wrapping key shared by the sending and receiving parties and decrypted using the same key.	NIST SP 800-57 Part 1 Rev. 5
key update	A function performed on a cryptographic key in order to compute a new key that is related to the old key and is used to replace that key. Note: NIST SP 800-57 Part 1 Rev. 5 disallows this method of replacing a key.	NIST SP 800-57 Part 1 Rev. 5
key wrapping	A method of cryptographically protecting keys using a symmetric key that provides both confidentiality and integrity protection.	NIST SP 800-57 Part 1 Rev. 5

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)	CNSSI No. 4005
KOA registration manager	The individual responsible for performing activities related to registering key management infrastructure operating accounts (KOAs).	
label	A short, fixed length, physically contiguous identifier, usually of local significance.	IETF RFC 5920
	Identifier that is attached to a set of data elements.	ISO/IEC 2382:2015
	See *security label*, *marking.*	
labeled security protections	Access control protection features of a system that use security labels to make access control decisions.	ITU-T X.500
latency	The delay in processing or in availability	NIST SP 1500 Vol 1 Rev. 3
lawful government purpose	Any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement).	32 CFR Vol 6 Part 2002.4
layered COTS product solutions	Commercial CS and CS-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).	CNSSP No. 11 (adapted)

	See *commercial solutions for classified (CSfC).*	
least privilege	A security principle that a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks.	NIST SP 800-57 Part 2 (adapted)
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.	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*.	CNSSI No. 4000 (adapted)
line conduction	Unintentional signals or noise induced or conducted on a telecommunications or automated information system signal, power, control, indicator, or other external interface line.	NSTISSI 7002
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.	
link encryption	The data security process of encrypting information at the data link level as it is transmitted between two points within a network.	Searchsecurity (adapted)
	Sometimes called "link level" or "link layer encryption". Contrast with *end-to-end encryption.*	

link encryption family cryptographic interoperability specification (LEF-CIS)	A standard defining the requirements for bulk data link encryption, similar to Ethernet and HAIPE encryption, but for Link Encryption Family devices.	
local access	Access to an organizational system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.	NIST SP 800-53 Rev. 5
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.	CNSSI No. 4005
local element	See *hand receipt holder*.	
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).	CNSSI No. 4005
local registration authority (LRA)	A registration authority with responsibility for a local community.	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.	FICAM Roadmap and Implementation Guidance V2.0
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 title of a COMSEC item that includes the name of the manufacturer followed by the equipment designator, a short functional description, and the model designator (e.g., Acme All Purpose Secure Radio Model APR-001).	CNSSI No. 4033
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).	FIPS 199
low-impact system	An information system in which all three security properties (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.	FIPS 200

	Note: For National Security Systems, CNSSI No. 1253 assigns one impact value (low, moderate, or high) for each of the three security objectives (confidentiality, integrity, and availability), rather than using the FIPS 200 high water mark across security objectives.	
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.	CNSSAM TEMPEST/1-13
low probability of detection (LPD)	Result of measures used to hide or disguise intentional electromagnetic transmissions.	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.	CNSSI No. 1200
low probability of positioning	Result of measures used to resist attempts by adversaries to determine the location of a particular transmitter.	CNSSI No. 1200
macro virus	A specific type of computer virus that is encoded as a macro embedded in some document and activated when the document is handled.	NIST SP 800-28 Ver. 2
magnetic remanence	Magnetic representation of residual information remaining on a magnetic medium after the medium has been cleared. See *clear* and *remanence*.	
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.	CNSSI No. 4005

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 communication systems, networks, physical or virtual infrastructure controlled by computers of information systems, or information resident thereon.	NSA/CSS Policy 11-11
malicious logic	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.	IETF RFC 4949 Ver 2
malware	See *malicious code* and *malicious logic*.	
manageability [privacy context]	Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure. See also *disassociability [privacy context]* and *predictability [privacy context]*.	NISTIR 8062
managed interface	An interface within a system that provides boundary protection capabilities using automated mechanisms or devices.	NIST SP 800-53 Rev. 5
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	Safeguards or countermeasures for an information system that focus on the management of risk and the management of system security.	FIPS 200 (adapted)
	Note: Sometimes called "program management controls"; contrast with *common controls, operational controls,* and *technical controls.*	

mandatory access control (MAC)	An access control policy that is uniformly enforced across all subjects and objects within a system. A subject that has been granted access to information is constrained from: passing the information to unauthorized subjects or objects; granting its privileges to other subjects; changing one or more security attributes on subjects, objects, the system, or system components; choosing the security attributes to be associated with newly created or modified objects; or changing the rules for 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. Mandatory access control is considered a type of nondiscretionary access control.	NIST SP 800-53 Rev. 5
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*.	
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*.	

maritime cyberspace	A global domain consisting of the interdependent networks of Information Technology (IT) infrastructure, Operational Technology (OT) infrastructure, resident data, the electromagnetic spectrum, and any telecommunications networks, computers, information and communications systems, and embedded processors, and controllers related to maritime processes and functions. See also *cyberspace*.	
marking	Visible tag, brand, mark, pictorial, or other informative matter, written, printed, stenciled, marked, embossed, or impressed on, or attached to, the packaging or container of a product.	ISO/IEC 21371:2018 (adapted from the definition for *label*)
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.	FIPS 201-2
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.	NIST SP 800-53A Rev. 4
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.	FIPS 200
media access control security (MACsec)	Provides interoperable cryptographically-based security for Ethernet. 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) and confidentiality (via encryption).	

media sanitization	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.	NIST SP 800-88 Rev. 1
memorandum of agreement (MOA)	Used to document agreements and execute or deliver support with or without reimbursement between any two or more parties. When a support agreement involves reimbursement, an MOA can be used to further detail terms and conditions in addition to the FS Form 7600A.	DoDI 4000.19 (adapted)
memorandum of understanding (MOU)	Used to document a mutual understanding between any two or more parties that does not contain an expectation of payment, and under which the parties do not rely on each other to execute or deliver on any responsibilities.	DoDI 4000.19 (adapted)
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.	NIST SP 800-63-3
	See *checksum*.	
message digest	The result of applying a hash function to a message. Also known as a "hash value" or "hash output".	NIST SP 800-107 Rev. 1
message indicator (MI)	Sequence of bits transmitted over a communications system for synchronizing cryptographic equipment.	
metadata	Information that describes the characteristics of data, including structural metadata that describes data structures (i.e., data format, syntax, semantics) and descriptive metadata that describes data contents (i.e., security labels).	NIST SP 800-53 Rev. 5
metrics	Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.	NIST SP 800-55

minimization [privacy context]	A privacy principle (FIPP) that limits an organization's creation, collection, use, processing, storage, maintaining, disseminating, or disclosing of PII to activities that are directly relevant and necessary to accomplish a legally authorized purpose, and to only maintain PII for as long as is necessary to accomplish the purpose.	OMB Circular A-130 (adapted)
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.	NIST SP 800-72
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.	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.	NIST SP 800-60 Vol 1 Rev. 1
mission-critical element	An element which is or contains information and communications technology (ICT), including hardware, software, or firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission critical functionality of a system of which, because of the system's design, may introduce vulnerability to a mission critical function of a system.	CNSSD No. 505 (adapted)
mission-critical function	Any function that, if compromised, would degrade the system effectiveness in achieving the core mission for which it was designed.	CNSSD No. 505 (adapted)

mission-specific enterprise cross domain service (MS-ECDS)	An enterprise cross domain service available to a select community [e.g., signals intelligence (SIGINT), geospatial intelligence (GEOINT), Maritime] with a limited set of data types and domains.	DISN CPG (adapted)
mission-specific enterprise cross domain service provider (MS-ECDSP)	An ECDSP providing an enterprise cross domain service that is available to a select community [e.g., signals intelligence (SIGINT), geospatial intelligence (GEOINT), Special Operations, Maritime] with a limited set of data types and security domains.	DISN CPG (adapted)
misuse of controlled unclassified information (CUI)	Any situation when someone uses controlled unclassified information (CUI) in a manner not in accordance with the policy contained in Executive Order 13556 (or any successor order), 32 Code of Federal Regulations (CFR), the CUI Registry, agency CUI policy, or the applicable laws, regulations, and Government-wide policies that govern the affected information. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI. This may also include designating or marking information as CUI when it does not qualify as CUI.	32 CFR 2002.4
mitigation	See *risk mitigation*.	
mobile code	Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.	NIST SP 800-53 Rev. 5
	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.	DoDI 8500.01

mobile code technologies	Software technologies that provide the mechanisms for the production and use of mobile code.	NIST SP 800-53 Rev. 5
mobile device	A portable computing device that has a small form factor such that: • it can easily be carried by a single individual; • is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); • possesses local, non-removable/removable data storage; and • includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, or built-in features that synchronize local data with remote locations. Examples include smartphones, tablets, and E-readers. Also known as a "portable computing device."	NIST SP 800-53 Rev. 5 (adapted)
	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.).	FIPS 199 (adapted)
moderate-impact system	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.	FIPS 200
	Note: For National Security Systems, CNSSI No. 1253 assigns one impact value (low, moderate, or high) for each of the three security objectives (confidentiality, integrity, and availability), rather than using the FIPS 200 high water mark across security objectives.	
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 system or keys.	CNSSI No. 4006

multifactor authentication (MFA)	A characteristic of an authentication system or an authenticator that requires more than one distinct authentication factor for successful authentication. MFA can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.	NIST SP 800-63-3
	Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). See *authenticator*.	NIST SP 800-171 Rev 2 (adapted)
	Note: the term "dual-factor authentication" describes a multifactor authentication schema where two factors of authentication are used. This was previously sometimes called "strong authentication".	
multi-level cross domain solution	A type of cross domain solution (CDS) that uses trusted security labeling to associate a classification or sensitivity level with objects and enforces a mandatory security policy over a subject's access to objects, based upon the security domain and authorization attributes.	CNSSI No. 1253F Attachment 3 (adapted)
multi-level device	Equipment trusted to properly maintain and separate data of different security domains.	
	A device that is used in a manner that permits it to simultaneously process data of two or more security levels without risk of compromise. To accomplish this, sensitivity labels are normally stored on the same physical medium and in the same form (i.e., machine-readable or human-readable) as the data being processed.	**NCSC-TG-004*
multi-level solution	A technical implementation of multi-level security.	DoDI 8540.01

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.	
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.	
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.	CNSSI No. 4003
national-essential functions	The select functions that are necessary to lead and sustain the United States during a catastrophic emergency and that, therefore, must be supported through COOP, COG, and ECG capabilities.	DoDD 3020.26

national information assurance partnership (NIAP)	A U.S. Government initiative managed by the National Security Agency, 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. 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 COTS CS and CS-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 Standard 15408-1:2009).	
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 (NSEP) 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), which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NSEP posture of the United States.	47 CFR Part 64 Appendix A (adapted)

national security information (NSI)	Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Unauthorized disclosure of NSI could reasonably be expected to cause identifiable or describable damage to national security. Note: Synonymous with classified information and classified national security information (CNSI).	E.O. 13526 (adapted)
	See *classified information, controlled unclassified 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).	Public Law 113-283
	Note: NIST SP 800-59 features a variety of questions to help determine whether a system may be designated a national security system.	
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).	https://nvd.nist.gov/

need-to-know	A determination within the executive branch in accordance with directives issued pursuant to this order [E.O. 13526] that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.	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.	
negative control (security)	Passive form of security monitoring where a specified action or event triggers an alarm; a lack of information indicates the item being monitored is secure.	
	Contrast with *positive control (security)*	
network	A system implemented with a collection of connected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices	NIST SP 800-53 Rev. 5
network access	Access to a system by a user (or a process acting on behalf of a user) communicating through a network, including a local area network, a wide area network, and the Internet.	NIST SP 800-53 Rev. 5

network defense	Programs and activities (including those governed by PPD-41), and the use of tools necessary to facilitate them, conducted on information systems, networks, or physical or virtual infrastructure by the owner or operator or with the consent of the owner or operator and, as appropriate, the user for the primary purpose of protecting (1) those information systems, networks, or physical or virtual infrastructure; or (2) data stored on, processed on, or transiting those information systems, networks, or physical or virtual infrastructure. Network Defense does not involve accessing or conducting activities on information systems, networks, or physical or virtual infrastructure without authorization from the owner or operator or exceeding access authorized by the owner or operator.	NSPM-13
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.	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.	
network time protocol	Used in networks of all types and sizes for time synchronization of servers, workstations, and other networked equipment.	IETF RFC 5907
next generation encryption (NGE)	An NSA portfolio of development programs to support the DoD's Cryptographic Modernization Initiative to modernize the NSA-certified cryptographic product inventory.	

NIAP product compliant list (PCL)	The list of CS and CS-enabled COTS products evaluated and validated pursuant to the National Information Assurance Partnership (NIAP) program. PCL products conform with Common Criteria for IT Security Evaluation (ISO/IEC Standard 15408-1:2009).	CNSSP No. 11 (adapted)
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)* and *two-person control (TPC)*.	
nonce	A random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing liveness and thus detecting and protecting against replay attacks.	IETF RFC 4949 Ver 2 (adapted)
non-discretionary access control	See *mandatory access control (MAC)*.	
nonlocal maintenance	Maintenance activities conducted by individuals who communicate through either an internal or external network	NIST SP 800-53 Rev. 5
non-organizational user	A user who is not an organizational user (including public users).	NIST SP 800-53 Rev. 5
non-person entity (NPE)	An entity related to information technology with a digital identity that acts in cyberspace, but is not a human actor. This can include organizations, hardware objects (physical entities/devices), software objects (virtual/logical entities), and information artifacts.	DHS OIG 11-121 (adapted) and ICS 500-30 (adapted)

non-repudiation	Protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message.	NIST SP 800-53 Rev. 5
NSA-approved commercial solution	The combination of multiple COTS CS 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.	CNSSAM IA-01-12 (adapted)
NSA-approved cryptography	Cryptography that consists of an approved algorithm, an implementation that has been approved for the protection of classified information and/or controlled unclassified information in a specific environment, and a supporting key management infrastructure.	NIST SP 800-53 Rev. 5
NSS baselines	The combination of applicable NIST SP 800-53 baselines and the security and privacy controls required for National Security System (NSS).	CNSSI No. 1253 (adapted)
nuclear command and control cryptographic material	Cryptographic 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.	NSA/CSS Policy 3-3 (adapted)
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 system-related entity, including bits, bytes, words, fields, devices, files, records, programs, tables, processes, programs, segments, directories, processors, and domains that contain or receive information. Access to an object (by a subject) implies access to the information it contains.	NIST SP 800-53 Rev. 5 (adapted)
	Note: Sometimes referred to as "resource"	

	See *subject*.	
object reuse	The reassignment to some subject of a storage medium (e.g., page frame, disk sector, magnetic tape) that contained one or more objects. To be securely reassigned, no residual data can be available to the new subject through standard system mechanisms.	**NCSC-TG-025*
	Note: Also known as "residual information protection"	
offensive cyberspace operations (OCO)	Missions intended to project power in and through cyberspace.	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.	6 CFR § 5.41
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).	NIST SP 800-49 (adapted)
one-way transfer	Permitting the flow of data to move in one direction only.	
one-way transfer device	A mechanism, usually implemented in hardware, which enforces a unidirectional data flow with varying degrees of assurance, typically referred to as a "data diode" although not exclusively implemented as such. A common example is a fiber optic isolator.	

open storage	Any storage of classified national security information outside of General Services Administration-approved storage 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.	CNSSI No. 4005 (adapted)
open vulnerability assessment language (OVAL)	A language for representing system configuration information, assessing machine state, and reporting assessment results.	NIST SP 800-126 Rev. 3
operational controls	Safeguards or countermeasures for a system that primarily are implemented and executed by people (as opposed to systems).	FIPS 200 (adapted)
	Contrast with *management controls*, *technical controls*, and *common controls.*	
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.	
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.	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)	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.	DoDD 5205.02E
	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.	ICS 700-1
optional modification	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).	CNSSI No. 4005

organization	An entity of any size, complexity, or positioning within an organizational structure (e.g., federal agencies, private enterprises, academic institutions, state, local, or tribal governments, or as appropriate, any of their operational elements). See *enterprise*.	NIST SP 800-37 Rev. 2 (FIPS 200 Adapted)
organizational registration authority (ORA)	Entity within the public key infrastructure (PKI) that authenticates the identity and the organizational affiliation of the users.	
organizational user	An organizational employee or an individual whom the organization deems to have equivalent status of an employee, including a contractor, guest researcher, or individual detailed from another organization. Policies and procedures for granting the equivalent status of employees to individuals may include need-to-know, relationship to the organization, and citizenship.	NIST SP 800-53 Rev. 5
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.	NIST SP 800-32 (adapted)
overlay	A specification of security or privacy 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.	OMB Circular A-130
	A specification of security controls, control enhancements, supplemental guidance, and other supporting information intended to complement (and further refine) security control baselines resulting in the initial security control set.	CNSSI No. 1253, Appendix F

overt channel	Communications path within a computer system or network designed for the authorized transfer of data. Compare with *covert channel*.	**NCSC-TG-004 (adapted)*
over-the-air key distribution (OTAD)	Providing electronic key via over-the-air rekeying, over-the-air key transfer, or cooperative key generation.	NAG-16F
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.	NAG-16F
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.	NAG-16F
over-the-network keying (OTNK)	A set of data items and messages (termed OTNK Service Messages) that a KMI-aware User Device processes to receive identity specific and possibly cryptographically protected KMI Products and Services contained in CMS packages.	
overwrite	Writing data on top of the physical location of data stored on the media.	NIST SP 800-88 Rev. 1
packet sniffer	Software that observes and records network traffic.	
page check	The verification of the presence of each required page in a physical publication.	CNSSI No. 4005
passive attack	An attack that does not alter systems or data. See also *active attack*.	
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.	IETF RFC 4949 Ver 2 (adapted)

patch	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.	ISO/IEC 19770-2:2015
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.	GAO-12-137
peer entity authentication	The corroboration that a peer entity in an association is the one claimed.	IETF RFC 4949 Ver 2
peer entity authentication service	A security service that verifies an identity claimed by or for a system entity in an association.	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 a system.	NIST SP 800-53 Rev. 5
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.	
periods processing	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.	IETF RFC 4949 Ver 2

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	An electronic identity that is 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 by different organizations (e.g. a Director of National Intelligence contractor who is also an Army reservist).	ICTS UIAS v2.1 (adapted)
personal identification number (PIN)	A secret that a claimant memorizes and uses to authenticate his or her identity.	FIPS 201-2 (adapted)
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). Synonymous with personal identity verification (PIV) card. Note: PIV requirements are defined in FIPS 201-2.	CNSSI No. 1300 (adapted); FIPS 201-2
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.	

personally identifiable information (PII)	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.	OMB Circular A-130
physically protected space (PPS)	The space inside one physically protected perimeter. Separate spaces of equal protection may be considered to be part of the same PPS if the communication links between them are provided sufficient physical protection.	CNSSI No. 5000 (adapted)
plain text	Data that is input to an encryption process.	IETF RFC 4949 Ver 2 (adapted)
	Intelligible data, the semantic content of which is available without using cryptographic techniques.	ISO/IEC 2382:2015 (under plaintext)
	See *clear text*.	
plan of action and milestones (POA&M)	A tool that identifies tasks that need 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.	OMB Memorandum 2-01;
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.	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.	DoDI 8500.01
point-to-point cross domain solution (CDS)	A CDS purchased, implemented, and managed within the authorization boundary of the organization's own network. A point-to-point CDS is unable to use an ECDSP.	DISN CPG (adapted)

policy	The representation of rules or relationships that makes it possible to determine if a requested access should be allowed, given the values of the attributes of the subject/entity, object/resource, and possibly environment conditions.	NIST SP 800-162 (adapted)
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.	NIST IR 7657
policy enforcement point (PEP)	A system entity that requests and subsequently enforces authorization decisions.	NIST IR 7657
port scan	A technique that sends client requests to a range of service port addresses on a host. *See probe.*	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 (CD) and cassette players/recorders, portable digital assistant, audio devices, watches with input capability, and reminder recorders.	ICS 700-1
portable storage device	A system component that can be inserted into and removed from a system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain nonvolatile memory).	NIST SP 800-171 Rev. 2
	See also *removable media*.	

positive control (security)	Active form of security monitoring where an unexpected result generates an alarm. Note: The unexpected result generates an alarm because a positive control test was executed against a registered data set in which the correct result is very well-known, but the expected result was not returned or observed.	
	Contrast with *negative control (security)*. Replaced "positive cyber defense."	
positive control material	Generic term referring to any material, system, or information (e.g. a sealed authenticator system or permissive action link) that require positive control-type security monitoring.	
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.	FIPS 199 (adapted)
precursor	A sign that an attacker may be preparing to cause an incident.	NIST SP 800-61 Rev. 2
	See *indicator*.	
predictability [privacy context]	Enabling of reliable assumptions by individuals, owners, and operators about PII and its processing by a system. See also *disassociability [privacy context]* and *manageability [privacy context]*.	NISTIR 8062
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 authorizing official (PAO)	A senior (federal) official or executive with the authority to oversee and establish guidance for the strategic implementation of CS 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).	DoDI 8500.01 (adapted)
privacy continuous monitoring	Maintaining ongoing awareness of privacy risks and assessing privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.	OMB Circular A-130
privacy continuous monitoring program	An agency-wide program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at an agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks.	OMB Circular A-130
privacy continuous monitoring strategy	Formal document that catalogs the available privacy controls implemented at an agency across the agency risk management tiers and ensures that the controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.	OMB Circular A-130
privacy control	The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.	OMB Circular A-130

privacy control assessment	The assessment of privacy controls to determine whether the controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks. Note: A privacy control assessment is both an assessment and a formal document detailing the process and the outcome of the assessment.	OMB Circular A-130
privacy control baseline	See *control baseline*.	
privacy control enhancement	See *control enhancement*.	
privacy impact assessment (PIA)	An analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. Note: A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.	OMB Circular A-130
privacy plan	A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.	OMB Circular A-130

privacy program plan	A formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.	OMB Circular A-130
privacy requirement	A specification for system/product/service functionality to meet stakeholders' desired privacy outcomes.	NIST Privacy Framework, V1.0
privacy risk	The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur.	NIST Privacy Framework, V1.0
privacy risk assessment	A privacy risk management sub-process for identifying and evaluating specific privacy risks.	NIST Privacy Framework, V1.0
privacy risk management	A cross-organizational set of processes for identifying, assessing, and responding to privacy risks.	NIST Privacy Framework, V1.0
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.	CNSSI No. 1300
privilege	A right that, when granted to an entity, permits the entity access and/or authorization to an otherwise restricted object, state, or resource. Note: Privileges represent the authorized behavior of a subject. They are defined by an authority and embodied in policy or rules.	NIST SP 800-162
privilege certificate manager (PCM)	The key management entity (KME) authorized to create the privilege certificate for another KME.	CNSSI No. 4005

privileged account	A system account with authorizations of a privileged user.	NIST SP 800-171 Rev. 2
privileged command	A human-initiated command executed on a system that involves the control, monitoring, or administration of the system, including security functions and associated security-relevant information.	NIST SP 800-53 Rev. 5
privileged process	A computer process that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary processes are not authorized to perform.	IETF RFC 4949 Ver 2
privileged user	A user that is authorized (and therefore, trusted) to have access to perform system control, monitoring, administration functions, or security-relevant functions that ordinary users are not authorized to perform.	IETF RFC 4949 Ver 2 (adapted)
probability of occurrence	See *likelihood of occurrence*.	
probe	A technique that attempts to access a system to learn something about the system.	
	See *port scan*.	
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).	CNSSI No. 1011
product compliant list (PCL)	See *NIAP product compliant list (PCL)*	
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.	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	Information that is classified as top secret (TS) information; communications security (COMSEC) information (excluding controlled cryptographic items when un-keyed or utilized with unclassified keys); restricted data (RD); special access program information (SAP); or sensitive compartmented information (SCI).	32 CFR § 2004.4
protected distribution system (PDS)	Wireline or fiber-optic distribution system used to transmit unencrypted classified national security information through an area of lesser classification or control. Note: "An area of lesser classification or control" refers to unencrypted classified national security information passing from, for example, an area cleared for Top Secret material to an area only cleared for Secret material or from a medium-threat area with greater physical security controls to a high-threat area with fewer physical security controls.	NSA/CSS Policy 3-12
protecting application	An application that controls access to protected resources	

protection philosophy	Informal description of the overall design of a 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.	**NCSC-TG-004 (adapted)*
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.	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.	
protective technologies	Special tamper-evident features, materials, and items employed for the purpose of detecting, delaying, and deterring attempts to compromise, modify, penetrate, extract, or substitute cryptographic and information processing equipment and keying material throughout its lifecycle including the secure shipping of these materials.	

protocol	A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. and A series of ordered computing and communication steps that are performed by two or more system entities to achieve a joint objective.	IETF RFC 4949 Ver 2
protocol adapter (PA)	A process that communicates with entities external to a system. Protocol adapters typically implement Open Systems Interconnection (OSI) model layers 5-7.	
provenance	The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include the personnel and processes used to interact with or make modifications to the system, component, or associated data.	NIST SP 800-53 Rev. 5
provisional security impact values	The initial or conditional impact determinations made until all considerations are fully reviewed, analyzed, and accepted in the subsequent categorization steps by appropriate officials.	NIST SP 800-60 (adapted)
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.	NIST SP 800-44 Rev. 2
	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 hypertext transfer protocol (HTTP) proxy used for Web access, and a simple mail transfer protocol (SMTP) proxy used for e-mail.	

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	A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing.	
	An assigned identity that is used to protect an individual's true identity.	
pseudorandom number generator (PRNG)	See *deterministic random bit generator (DRBG)*.	
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 encrypt data or to verify signatures created with its corresponding private key.	CNSSI No. 1300 (adapted)
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.	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 by applying physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.	NIST SP 800-88 Rev. 1
purpose specification and use limitation [privacy context]	A privacy principle (FIPP) that addresses an organization's notice to individuals regarding the specific purpose for which PII is collected and restricting an organization's use, processing, storage, maintenance, dissemination, or disclosure of PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.	OMB Circular A-130 (adapted)
quadrant	Short name referring to technology that provides tamper-resistant protection to cryptographic equipment.	
quality and integrity [privacy context]	A privacy principle (FIPP) that limits an organization's data processing activities to those that meet standards of accuracy, relevance, timeliness, and completeness that are reasonably necessary to ensure fairness to the individual.	OMB Circular A-130 (adapted)
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 bit generator (RBG) seed	A string of bits that is used to initialize a DRBG. Also called a "seed." See *seed*.	NIST SP 800-57 Part 1 Rev. 5
random number generator (RNG)	A process that generates a random sequence of values (usually a sequence of bits) or an individual random value. Uses one or more non-deterministic bit sources and a processing function that formats the bits, and outputs an unpredictable and uniformly distributed sequence of values. Note: An RNG is also considered a randomizer.	IETF RFC 4949 Ver 2 (adapted)
real time reaction (C.F.D.)	Immediate response to a penetration attempt that is detected and diagnosed in time to prevent access.	
reciprocity	Agreement among participating organizations to accept each other's security assessments to reuse system resources and/or to accept each other's assessed security posture to share information.	NIST SP 800-37 Rev. 2
reconstitution	Follows recovery operations during contingency plan execution. Includes activities to return organizational systems to fully operational states; the deactivation of any interim system capabilities needed during recovery operations; assessments of fully restored system capabilities; reestablishment of continuous monitoring activities; potential system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures.	NIST SP 800-53 Rev. 5 (adapted)
recovery	Recovery is executing system contingency plan activities to restore organizational missions/business functions.	NIST SP 800-53 Rev. 5 (adapted)
recovery and reconstitution	Actions taken during or after an incident or event to restore functions and capability to fully operational states.	NIST SP 800-53 Rev. 5 (adapted); DOD Dictionary (as amended) (adapted)

	Reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Associated capabilities can include both automated mechanisms and manual procedures. See: *reconstitution, recovery*.	NIST SP 800-53 Rev. 5 (adapted)
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 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).	NIST SP 800-171 Rev. 2
recovery procedures	The actions necessary to restore a system's computational capability and data files after a system failure.	**NCSC-TG-004*
RED	Information or messages that contain sensitive or classified information that is not encrypted. See also *BLACK*.	
RED/BLACK concept	Separation of electrical and electronic circuits, components, equipment, and systems that handle classified plain text (RED) information, in electrical signal form, from those that handle unclassified (BLACK) information in the same form.	NSA/CSS Policy 3-12
RED data	Data that is not protected by encryption.	CNSSI No. 4005 (adapted)
RED equipment	A term applied to equipment that processes unencrypted national security information that requires protection during electrical/electronic processing.	CNSSAM TEMPEST/1-13

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*.	CNSSI No. 4005
RED line	An optical fiber or a metallic wire that carries a RED signal or that originates/terminates in a RED equipment or system.	CNSSAM TEMPEST/1-13
RED optical fiber line	An optical fiber that carries RED signal or that originates/terminates in RED equipment or system.	CNSSAM TEMPEST/1-13
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.	CNSSAM TEMPEST/1-13
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 CS by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.	
RED wireline	A metallic wire that carries a RED signal or that originates/terminates in a RED equipment or system.	CNSSAM TEMPEST/1-13
registration	The act of collecting the information needed from an entity to issue that entity a credential.	FICAM Services Framework

registration authority (RA)	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.	CNSSI No. 1300
	The key management entity (KME) within each Service or Agency responsible for registering KMEs and assigning electronic key management system (EKMS) IDs to them.	CNSSI No. 4005
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.	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.	CNSSI No. 1300
remanence	Residual information remaining on storage media after clearing. See *clear* and *magnetic remanence.*	IETF RFC 4949 Ver 2 (adapted)
remediation	Actions taken to correct known deficiencies and weaknesses once a vulnerability has been identified.	DoDD 3020.40
	The act of mitigating a vulnerability or a threat.	

remote access	Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network.	NIST SP 800-53 Rev. 5
remote maintenance	Maintenance activities conducted by individuals communicating through an external network.	NIST SP 800-53 Rev. 5
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; external/removable hard drives; external/removable solid-state disc drives; magnetic/optical tapes; flash memory devices; flash memory cards; and all other external/removable disks.	
	See also *portable storage device*.	
removable media device	See *portable storage device*.	
replay attack	An attack in which the attacker is able to replay previously captured messages (between a legitimate claimant and a verifier) to masquerade as that claimant to the verifier or vice versa.	NIST SP 800-63-3
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.	CNSSI No. 4005
residual risk	Portion of risk remaining after security measures have been applied.	**NIST SP 800-33 (adapted*

residue	Data left in storage after information processing operations are complete, but before degaussing or overwriting has taken place.	**NCSC-TG-004 (adapted)*
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.	PPD-21
resource	A device, data element, or file for which access is requested. Also known as protected resource and as an object.	XACML 3.0 (adapted)
resource negotiation	Built-in data management capabilities that provide the necessary support functions, such as operations management, workflow integration, security, governance, support for additional processing models, and controls for multi-tenant environments, providing higher availability and lower latency applications.	NIST SP 1500 Vol 1 Rev 3
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.	CNSSI No. 1300
reusability	The ability to use a system, system component, or data for a different purpose or to achieve a different goal than originally intended.	
revocation	The process of permanently ending the binding between a certificate and the identity asserted in the certificate from a specified time forward.	CNSSI No. 1300

risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.	OMB Circular A-130
risk acceptance	The appropriate risk response when the identified risk is within the organizational risk tolerance	NIST SP 800-39
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	A systematic examination of risk using disciplined processes, methods, and tools. A risk assessment provides an environment for decision makers to evaluate and prioritize risks continuously and to recommend strategies to remediate or mitigate those risks.	DoDD 3020.40
	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	NIST SP 800-30 Rev. 1
	See *assessment [general context]*	
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.	NIST SP 800-30 Rev. 1
risk assessor	The individual, group, or organization responsible for conducting a risk assessment.	NIST SP 800-30 Rev. 1

risk avoidance	The appropriate risk response when the identified risk exceeds the organizational risk tolerance.	NIST SP 800-39
risk executive (function)	An individual or group within an organization, led by the senior accountable official for risk management, that helps to ensure that security risk considerations for individual 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 managing risk from individual systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.	NIST SP 800-37 Rev. 2
risk framing	Establishing the context for risk-based decisions.	NIST SP 800-39 (adapted)
risk management	The program and supporting processes to manage risk to organizational operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and - includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.	OMB Circular A-130 (adapted)
risk management framework (RMF)	A disciplined and structured process that integrates information security, privacy, and risk management activities into the system development life cycle (SDLC).	OMB Circular A-130 (adapted)
	The RMF is described in NIST SP 800-37 Rev. 2	

risk management framework (RMF) data elements	A basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Standardization of data elements documented within the RMF core documents facilitates reciprocity. These data elements may be mapped to other security documentation to avoid duplication of efforts (e.g., test and evaluation, program protection profiles, engineering documents).	CNSSI 1254 (adapted)
risk mitigation	The appropriate risk response for that portion of risk that cannot be accepted, avoided, shared, or transferred; also called risk reduction.	NIST SP 800-39
	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.	
	See also *safeguards*, *countermeasure*, *recovery & reconstitution*, and *remediation.*	
risk mitigation plan (RMP)	A plan that describes the risks to a mission arising from an asset's operational factors and the decisions that balance risk cost with mission benefits.	DoDD 3020.40
risk response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations, organizational assets, individuals, other organizations, or the Nation.	OMB Circular A-130 (adapted)
	Actions taken to remediate or mitigate risk or reconstitute capability in the event of loss or degradation.	DODD 3020.40
risk tolerance	Levels and types of risk that are acceptable.	NIST SP 800-30
risk transfer	The appropriate risk response when organizations desire and the means to shift the entire responsibility/liability from one organization to another.	NIST SP 800-39
robustness	The ability of a CS entity to operate correctly and reliably across a wide range of operational conditions, and to fail gracefully outside of that operational range.	

role	Predefined set of rules establishing the allowed interactions between a user and a system.	ISO/IEC 15408-1:2009 (adapted)
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.	NIST SP 800-53 Rev. 5
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.	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	See *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.	FIPS 200

safety critical system	A system whose failure, malfunction, design flaw, or manufacturing flaw may result in one (or more) of the following outcomes: loss of life, serious injury to people, environmental damage/destruction, or loss or severe damage to equipment/property.	
salt	A non-secret value used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker.	NIST SP 800-63-3
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	A process to render access to target data on the media infeasible for a given level of effort. Clear, Purge, Damage, and Destroy are actions that can be taken to sanitize media.	NIST SP 800-88 Rev. 1
	The removal of extraneous or potentially harmful data (e.g., malware) within a file or other information container (e.g., network protocol packet).	
	The removal of information from the storage device such that data recovery using any known technique or analysis is prevented. Sanitization includes the removal of data from the storage device, as well as the removal of all labels, markings, and activity logs. The method of sanitization varies depending upon the storage device in question, and may include degaussing, incineration, shredding, grinding, embossing, etc.	NSA/CSS Policy Manual 9-12
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.	**NCSC-TG-004 (adapted)*

schema	An object's defined organization and structure, including the syntax, semantics, and metadata about each field in the structure.	
scoping considerations	A part of tailoring guidance that provides organizations with specific considerations on the applicability and implementation of security and privacy controls in the control baselines. Considerations include policy or regulatory, technology, physical infrastructure, system component allocation, public access, scalability, common control, operational or environmental, and security objective	NIST SP 800-53 Rev. 5
secret key	See *symmetric key*.	NIST SP 800-57 Part 1 Rev. 5
secret-key algorithm	See *symmetric-key algorithm*.	NIST SP 800-57 Part 1 Rev. 5
secure association key (SAK)	The secret key used by a MACsec Secure Assocation (SA).	
secure channel (SC)	A MACsec security relationship used to provide security guarantees for frames transmitted from one member of a Connectivity Association (CA) to the others. An SC is supported by a sequence of Secure Associations (SAs) thus allowing the periodic use of fresh keys without terminating the relationship.	
secure communication protocol	A communication protocol that provides the appropriate confidentiality, source authentication, and integrity protection.	NIST SP 800-57 Part 1 Rev. 5
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.	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.	FIPS 180-4 (adapted)
secure sockets layer (SSL)	A protocol used for protecting private information during transmission via the Internet.	*NIST SP 800-63-3 (adapted)*
	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	State in which the system's data are consistent and the system continues correct enforcement of security and privacy controls.	ISO/IEC 15408-1:2009 (adapted)
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).	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 [privacy context]	A privacy principle (FIPP) that addresses establishing administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm to individuals that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.	OMB Circular A-130 (adapted)
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.	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 that represents the basic properties or characteristics of an entity with respect to safeguarding information. Typically associated with internal data structures — including records, buffers, and files within the system — and 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.	NIST SP 800-53 Rev. 5

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.	CNSSI No. 1300
security authorization (to operate)	See *authorization to operate (ATO)*.	
security banner	A persistent visible window on a computer monitor that displays the highest level of data accessible during the current session.	
	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.	FIPS 199 (adapted)
security categorization	The process of determining the security category for information or a system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems. See *security category*.	NIST SP 800-53 Rev. 5
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.	NIST SP 800-126 Rev. 3

	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	See *control assessment.*	
security control assessor (SCA)	See *control assessor*.	
security control baseline	See *control baseline.*	
security control enhancements	See *control enhancement*.	
security control extension	A statement, used in security control overlays, that extends the basic capability of a security control by specifying additional functionality, altering the strength mechanism, or adding or limiting implementation options.	CNSSI No. 1253
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.	FIPS 199
security domain	A domain operating at a single security level (which includes a unique combination of classification, releasabilities, and dissemination controls) that implements a security policy and is administered by a single authority.	CNSSP No. 24 (adapted)
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.	**NCSC-TG-004 (adapted)*
security filter	A secure subsystem of an information system that enforces security policy on the data passing through it.	**NCSC-TG-004 (adapted)*
security impact analysis	The analysis conducted by an organizational official to determine the extent to which a change to an information system has affected the security state of that system.	NIST SP 800-128 (adapted)
security incident	See *incident*.	
security inspection	See *inspection.*	
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.	**DoD 5200.28-STD (adapted)*
security label	A piece of information that represents the security level of an object.	**NCSC-TG-004*
	The means used to associate a set of security attributes with a specific information object as part of the data structure for that object.	NIST SP 800-53 Rev. 5
	See *label.*	
security level	Includes the combination of classification level, releasability, and dissemination controls (e.g., sensitive compartmented information (SCI) compartment(s), special access program (SAP) identifier(s), alternative compensatory control measures (ACCM) nickname(s)) for an object or system.	

security marking	The means used to associate a set of security attributes with objects in a human-readable form in order to enable organizational, process-based enforcement of information security policies.	NIST SP 800-53 Rev. 5
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 or privacy-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 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.	
	The boundary where security controls are in effect to protect assets.	*NCSC-TG-004
security plan	A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. See *system security plan* or *information security program plan*.	OMB Circular A-130
security policy	A set of criteria for the provision of security services.	NIST SP 800-53 Rev. 5
	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.	*NCSC-TG-004
security posture	The security status of an enterprise's networks, information, and systems based on CS 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	See *system security plan* or *information security program plan*.	
security protocol	An abstract or concrete protocol that performs security-related functions.	
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*.	**NCSC-TG-004*
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).	
	Any event that attempts to change the security state of the system, (e.g., change discretionary access controls, change the security level of the subject, change user password, etc.). Also, any event that attempts to violate the security policy of the system, (e.g., too many attempts to login, attempts to violate the mandatory access control limits of a device, attempts to downgrade a file, etc.).	*DoD 5200.28-STD**
	See *event.*	
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.	FIPS 200
security requirements baseline	Description of the minimum requirements necessary for an information system to maintain an acceptable level of risk.	**NCSC-TG-004*

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.	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.	**NCSC-TG-004*
security service	A capability that supports one, or many, of the security goals. Examples of security services are key management, access control, and authentication.	NIST SP 800-160 (adapted)
	A processing or communication service that is provided by a system to give a specific kind of protection to resources, where said resources may reside with said system or reside with other systems, for example, an authentication service or a PKI-based document attribution and authentication service. A security service is a superset of AAA services. Security services typically implement portions of security policies and are implemented via security mechanisms.	NIST SP 800-95
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.	CNSSI No. 1300 (adapted)
security target	Implementation-dependent statement of security needs for a specific identified target of evaluation (TOE).	ISO/IEC 15408-1:2009 (adapted)

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.	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.	**NCSC-TG-004*
seed	A secret value that is used to initialize a process [e.g., a deterministic random bit generator (DRBG)]. See *RBG seed*.	NIST SP 800-57 Part 1 Rev. 5 (adapted)
self-encrypting devices (SED)	A data storage device featuring always-on encryption that substantially reduces the likelihood that unencrypted data is inadvertently retained on the device.	NIST SP 800-88 Rev. 1, page 9 (adapted)
senior agency information security officer (SAISO)	Official responsible for carrying out the chief information officer (CIO) responsibilities under the Federal Information Security Modernization Act (FISMA) and serving as the CIO's primary liaison to the agency's authorizing officials, information system owners, and information systems security officers.	FIPS 200
	Note: Also known as *senior information security officer (SISO)* or *chief information security officer (CISO)*.	
senior agency official for privacy (SAOP)	The senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.	OMB Circular A-130

senior information security officer (SISO)	See *senior agency information security officer (SAISO)*.	
sensitive compartmented information (SCI)	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.	ICD 703
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).	ICS 700-1
sensitive information	See *controlled unclassified information (CUI)*.	
sensitivity	A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.	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.	CNSSI No. 4005
service level agreement (SLA)	Defines the specific responsibilities of the service provider and sets the customer expectations.	

service of common concern	A service deemed to be more efficiently or effectively accomplished in a consolidated manner that is developed and maintained on behalf of the Intelligence Community by one or more Intelligence Community elements designated by the Director of National Intelligence, in consultation with affected heads of departments or Intelligence Community elements.	E.O. 12333, as amended (adapted)
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.	CNSSI No. 4033 (adapted)
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.	CNSSI No. 4005
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.	CNSSAM TEMPEST/1-13
signature [general context]	A recognizable, distinguishing pattern.	NIST SP 800-61 Rev. 2 (adapted)
	See also *digital signature*, *attack signature*.	
signature [cybersecurity context]	A specific sequence of events indicative of an unauthorized access attempt.	**NIST SP 800-12 (under attack signature)*
	A text string (algorithm or expression), used to configure intrusion detection systems and sensors, describing characteristics, patterns or other identifying information of cyber threat activity.	NSA/CSS Policy 11-11

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.	NIST SP 800-32 (adapted)
significant consequences	Loss of life or serious injury; serious damage to significant property; serious adverse foreign policy consequences to United States National Interests; or significant economic harm.	NSPM-13
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	An implementation of a data-centric architecture where essential data management metadata is associated and maintained for individual data objects/data records. Such data objects are "self-describing" making them more readily sharable across IT systems while still ensuring their appropriate protection and handling. What is considered essential data management metadata can vary based on an enterprise's needs, but typically encompasses metadata describing the authorities under which the data is managed, security access controls, data use policy, data handling, data retention, and data source provenance information.	
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.	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. See *firmware* and *hardware*.	IETF RFC 4949 Ver 2
software assurance (SwA)	The level of confidence that software is free from vulnerabilities - either intentionally designed into the software or accidentally inserted during its lifecycle - and functions in the intended manner.	NIST SP 800-163 Rev. 1
	The planned and systematic set of activities that ensure that software life cycle processes and products conform to requirements, standards, and procedures.	NASA-STD 8739.8
software identification (SWID) tag	Information structure containing identification information about a software configuration item, which may be authoritative if provided by a software creator.	ISO/IEC 19770-25:2015
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.	**NCSC-TG-004*
spam	Electronic junk mail.	IETF RFC 4949 Ver 2
	The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.	NIST SP 800-53 Rev. 5
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.	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.	DoDM 5205.07, Vol. 4
special category	Sensitive compartmented information (SCI), special access program (SAP) information, or other compartment information.	CNSSAM TEMPEST/1-13
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: ' -! @ # $ % /\ & * ( ) _ + I } { " : ? > < [ ] \ ; ' , . / - =	
spillage	Security incident that results in the transfer of classified information or Controlled Unclassified Information onto an information system not authorized to store or process that information.	
split knowledge	A process by which a cryptographic key is split into *n* key shares each of which provides no knowledge of the key. The shares can be subsequently combined to create or recreate a cryptographic key or to perform independent cryptographic operations on the data to be protected using each key share. If knowledge of *k* (where *k* is less than or equal to *n*) shares is required to construct the key, then knowledge of any *k* - 1 key shares provides no information about the key other than, possibly, its length.	NIST SP 800-57 Part 1 Rev. 5
spoofing	An attempt to gain access to a system by posing as an authorized user. Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.	**NCSC-TG-004 (adapted)*

spread spectrum	Telecommunications techniques in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information. Note: 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.	NIST SP 800-53 Rev. 5
steganography	The art, science, and practice of communicating in a way that hides the existence of the communication.	NIST SP 800-72 (adapted)
steward	A privileged person entity responsible for curating ICAM data.	
stream cipher	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. Note: Common types of ciphers are stream and block ciphers, which each have unique strengths and weaknesses. Ciphers are often separated by types of keys into asymmetric and symmetric key algorithms.	Handbook of Applied Cryptography
strength of mechanism (SML)	A scale for measuring the relative strength of a security mechanism hierarchically ordered from SML 1 through SML 3.	IATF Release 3.1, Appendix B
striped core	See *black transport.*	
subaccount	A COMSEC account that only received key from, and only reports to, its parent account, never a Central Office of Record.	CNSSI No. 4005

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.	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.	CNSSI No. 4005
subject	The entity requesting to perform an operation upon an object. See *object*.	NIST SP 800-162
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*.	NIST SP 800-32 (adapted)
subscriber	A party who has received a credential or authenticator from a Credential Service Provider.	NIST SP 800-63-3
Suite A	See *confidential algorithm.*	
Suite B	See *commercial national security algorithm (CNSA).*	
superencryption	An encryption operation for which the plaintext input to be transformed is the ciphertext output of a previous encryption operation.	IETF RFC 4949 Ver 2
	The encrypting of already encrypted information.	
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.	NIST SP 800-32 (adapted)
	See *subordinate certification authority*.	

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.	NIST SP 800-82 Rev. 2
supply chain	A linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.	OMB Circular A-130
	Network that designs, manufactures, imports, distributes, and sells a product.	ISO 10377:2013
supply chain assurance	Confidence that the supply chain will produce and deliver elements, processes, and information that function as expected.	NIST IR 7622
supply chain attack [cybersecurity context]	An incident where an adversary exploits vulnerabilities in the product or service supply network of the intended target. Note 1: Supply chain attacks may be conducted at any point in a system lifecycle to exfiltrate or manipulate data, disrupt or manipulate system operations, or provide an adversary the ability to access, disrupt, or manipulate a system in the future. Note 2: The supply network of a product or service may be internal to a targeted organization (e.g. logistics services), or external (e.g. third-party product/service providers).	

supply chain risk [cybersecurity context]	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	OMB Circular A-130
	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 (referenced from The Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Section 806).	CNSSD No. 505 (adapted)
supply chain risk management (SCRM) [cybersecurity context]	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 supplied product and its sub-elements, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).	CNSSD No. 505
	The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information and communications technology product and service supply chains.	OMB Circular A-130
	Note: Also known as "information and communication technology (ICT) supply chain risk management (SCRM)" or "cyber-supply chain risk management (C-SCRM)"	
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).	CNSSI No. 1300
symmetric key	A single cryptographic key that is used with a symmetric-key cryptographic algorithm, is uniquely associated with one or more entities, and is not made public (i.e., the key is kept secret). A symmetric key is often called a secret key. 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	NIST SP 800-57 Part 1 Rev. 5 (adapted)
	Note: *Symmetric key* and *secret key* are synonymous terms.	
symmetric-key algorithm	A cryptographic algorithm that uses the same secret key for an operation and its complement (e.g., encryption and decryption). Also called a "secret-key algorithm."	NIST SP 800-57 Part 1 Rev. 5
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. Note: Systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.	
	Entity consisting of interdependent components.	ISO 3676:2012
	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 CS policy and procedures.	
system component	A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware.	NIST SP 800-171 Rev. 2
system development life cycle (SDLC)	See *system life cycle*	
system high	Highest security level supported by an information system.	

system high security mode	The mode of operation in which system hardware/software is only trusted to provide need-to-know protection between users. In this mode, the entire system, to include all components electrically and/or physically connected, must operate with security measures commensurate with the highest classification and sensitivity of the information being processed and/or stored. All system users in this environment must possess clearances and authorizations for all information contained in the system. All system output must be clearly marked with the highest classification and all system caveats, until the information has been reviewed manually by an authorized individual to ensure appropriate classifications and caveats have been affixed. A system is operating in the system-high mode when each user with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts has all of the following: a. A valid personnel clearance for all information on the system. b. Formal access approval for, and has signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs). c. A valid need-to-know for some of the information contained within the system.	**NCSC-TG-004 (adapted)*
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.	**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.	NIST SP 800-47
system life cycle	Period that begins when a system is conceived and ends when the system is destroyed.	ISO/IEC 24765:2017 (adapted)
	Note 1: Often used synonymously with "system development life cycle (SDLC)", and sometimes defined with formalized steps (e.g. planning, analysis, design, implementation, and maintenance). Note 2: Those responsible for the security of a system will likely not have responsibility for the system throughout its entire life cycle, but should recognize the kinds of risks that may emanate from those areas of the lifecycle outside of their purview (e.g. supply chain risks or post-retirement risks).	
system low	The lowest security level supported by a system at a particular time or in a particular environment.	**NCSC-TG-004*
system or device certificate	A system or device certificate contains a system or device name as the subject. Note: Examples of systems or devices are workstations, guards, firewalls, routers, web server, database server, and other infrastructure components.	CNSSI No. 1300
system owner	An organizational official (or the organization itself) responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system.	NIST SP 800-37 Rev. 2 (adapted)
system owner [FISMA/RMF context]	An organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system.	NIST SP 800-37 Rev. 2
systems security engineer	Individual assigned responsibility for conducting system security engineering activities.	NIST SP 800-37 Rev. 2

systems security engineering (SSE)	Process that captures and refines security requirements and ensures their integration into information technology component products and information systems through purposeful security design or configuration.	NIST SP 800-37 Rev. 2
	Systems security engineering is a specialty engineering discipline of systems engineering that applies scientific, mathematical, engineering, and measurement principles, concepts, and methods to coordinate, orchestrate, and direct the activities of various security engineering specialties and other contributing engineering specialties to provide a fully integrated, system-level perspective of system security.	NIST SP 800-160, Volume 1
system security officer (SSO)	Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.	NIST SP 800-37 Rev. 2
	See *information system security officer (ISSO)*	
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.	NIST SP 800-18 Rev. 1
system service	A capability provided by a system that facilitates information processing, storage, or transmission.	NIST SP 800-53 Rev. 5 (from term information system service)
system-specific security control	A security or privacy control for an information system that is implemented at the system level and is not inherited by any other information system.	OMB Circular A-130

tactical cross domain solution (CDS)	A CDS that operates in austere environment conditions or environments where terrestrial communications are not possible. Austere environment conditions include combat and intelligence, surveillance, and reconnaissance (ISR) land, sea, or air vehicles. Terrestrial communications include direct connection to a telecommunications provider via electrical or optical cables, or the use of microwave, radio, or satellite communications. CDSs used in safety-critical environments or CDSs used for direct connection between sensor and shooter (e.g., missile, gun) can also be categorized as tactical.	DISN CPG (adapted)
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. Note: This term is used in a Department of Defense context.	
tailoring	The process by which security control baselines are modified by identifying and designating common controls; applying scoping considerations; selecting compensating controls; assigning specific values to agency-defined control parameters; supplementing baselines with additional controls or control enhancements; and providing additional specification information for control implementation. Note: The tailoring process may also be applied to privacy controls.	OMB Circular A-130
tampering	An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data.	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.	
	Set of software, firmware and/or hardware possibly accompanied by guidance.	Common Criteria
	Note: The TOE may be an IT product, a part of an IT product, a set of IT products, a unique technology that may never be made into a product, or a combination of these.	
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.	CNSSP No. 11
technical controls	Hardware and software controls used to provide automated protection to the IT system or applications. Technical controls operate within the technical system and applications.	NIST SP 800-16 (from the term "technical security controls")
	Safeguards or countermeasures that are primarily implemented and executed by a system through mechanisms contained in the hardware, software, or firmware components of the system.	FIPS 200 (adapted)
	Contrast with *management controls*, *operational controls*, and *common controls*.	
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 material	Equipment, components, devices, and associated documentation or other media which pertain to cryptography, or to the security of telecommunications and information systems.	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.	DoDI 5240.05
technical vulnerability information	A hardware, firmware, communication, or software flaw that leaves a computer processing system open for potential exploitation, either externally or internally, thereby resulting in risk for the owner, user, or manager of the system.	**NCSC-TG-004*

	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.	CNSSI No. 4005; NSTISSD 501
telecommunications security (TSEC) nomenclature	The National Security Agency (NSA) system for identifying the type and purpose of certain items of COMSEC material.	CNSSI No. 4005
TEMPEST	A name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment.	**FIPS 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.	CNSSAM TEMPEST/1-13
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.	CNSSI No. 4005
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.	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.	NIST SP 800-30 Rev. 1
threat event	An event or situation that has the potential for causing undesirable consequences or impact.	NIST SP 800-30 Rev. 1

	NIST SP 800-30 Rev. 1 Appendix E provides a representative list of threat events including, for example, communications interception attacks, counterfeit certificates, Denial of Service (DoS) attacks, phishing attacks, unauthorized access, etc.	
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 trigger a vulnerability. Synonymous with "threat agent".	FIPS 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.	CNSSI No. 4005

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.	CNSSI No. 4005
	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	
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).	CNSSI No. 4005
	Note: Some Tier 2 accounts or subaccounts operate a local management device (LMD) without a KP.	

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).	CNSSI No. 4005
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	See *authenticator*	
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.	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.	CNSSI No. 4005
traffic padding	Countermeasure that generates spurious data in transmission media to make traffic analysis or decryption more difficult	ISO/IEC 2382:2015
	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.	CNSSI No. 4005

transfer cross domain solution	A type of cross domain solution (CDS) that enforces security policy for the movement of data between information systems operating in different security domains.	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).	CNSSI No. 4005
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.	CNSSI No. 4005
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.	IETF RFC 8446 (adapted)
tranquility	Property whereby the security level of an object cannot change while the object is being processed by an information system.	**NCSC-TG-004 (adapted)*
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.	
transparency [privacy context]	A privacy principle (FIPP) that addresses an organization's practices for conveying information regarding policies and practices with respect to PII, and providing clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.	OMB Circular A-130
trap door [cryptography context]	A means of reading cryptographically protected information by the use of private knowledge of weaknesses in the cryptographic algorithm used to protect the data.	
	One-to-one function that is easy to compute in one direction, yet believed to be difficult to invert without special information.	

trap door [security context]	See *back door*.	
trigger	A set of logic statements to be applied to a data stream that produces an alert when an anomalous incident or behavior occurs.	CNSSD No. 504
	Event that causes the system to initiate a response. Note: Also known as "triggering event".	ISO/IEC 27031:2011
triple data encryption algorithm (TDEA)	An approved cryptographic algorithm that specifies both the DEA cryptographic engine employed by TDEA and the TDEA algorithm itself.	NIST SP 800-67 Rev. 2 (adapted)
triple DES (3DES)	See *triple data encryption algorithm (TDEA).*	
trojan horse	A computer program containing an apparent or actual useful function that also contains additional functions that permit the unauthorized collection, falsification, or destruction of data.	NIST SP 800-47
trust anchor	A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g. in a public key certificate). A trust anchor may have name or policy constraints limiting its scope.	NIST SP 800-63-3
	See *trusted certificate.*	
trust list	Collection of trusted certificates used by Relying Parties to authenticate other certificates.	NIST SP 800-32
trusted agent (TA)	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.	CNSSI No. 1300
	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.	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."	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.	
	A means by which two systems can communicate with necessary security and privacy assurances.	ISO/IEC 15408-1:2009 (adapted)
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.	**NCSC-TG-004 (adapted)*
trusted foundry	Facility that produces integrated circuits with a higher level of integrity assurance. Note: Defense Microelectronics Activity (DMEA) currently manages the DoD Trusted Foundry Program which accredits suppliers as "trusted".	
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.	CNSSI No. 1253
trusted path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the 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 system and cannot be imitated by untrusted software.	NIST SP 800-53 Rev. 5

trusted process	Process that has been tested and verified to operate only as intended or expected by the user.	
trusted recovery	A verified and validated process to restore system functionality to a known state after a system failure.	
trusted timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.	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.	NIST SP 800-37 Rev. 2
trustworthiness (system)	The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats and individuals' privacy.	NIST SP 800-37 Rev. 2
TSEC nomenclature	The NSA system for identifying the type and purpose of certain items of COMSEC material.	CNSSI No. 4005
tunneling	Encapsulation of one protocol's packet within the payload of another protocol's packets.	ISO/IEC 14908-4:2012
	Note: Tunneling enables one network to send its data via another network's connections.	
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.	DoDI 5200.44
	Note: Per NIST SP 800-53 Rev. 5, two-person control is also known as "dual authorization."	
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.	CNSSI No. 4005
	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.	

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.	**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.	
United States Computer Emergency Readiness Team (US-CERT)	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.	
U.S. national interests	Matters of vital interest to the United States, including national security, economic security, public safety, the safe and reliable functioning , and the availability of key resources.	NSPM-13
U.S. person	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.	22 CFR 120.15
	A citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).	50 U.S.C. Sec 1801
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.	NSTISSI 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.	NSTISSI 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.	CNSSI No. 4005
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.	NIST SP 800-57 Part 4
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)*, *national security information*, and *classified 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").	CNSSI No. 4005
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).	CNSSI No. 4005
unique identifier (UID)	A numeric or alphanumeric string that is exclusively associated with a single entity.	

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.	**NCSC-TG-004*
update (a certificate)	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.	NIST SP 800-32
	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.	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.	
user	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*.	CNSSI No. 4005
	Individual, or (system) process acting on behalf of an individual, authorized to access a system. See *organizational user* and *non-organizational user*.	NIST SP 800-53 Rev. 5
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.	CNSSD No. 504
user ID	A unique symbol or character string used by an information system to identify a specific user.	**NCSC-TG-004*
user representative	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)).	CNSSI No. 4005 (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	An activity that measures that a stakeholder's true needs and expectations are met.	ISO/IEC 24765:2017 (adapted)
	Contrast with *verification*	
variability	Changes in dataset, whether data flow rate, format/structure, semantics, and/or quality that impact the analytics application.	NIST SP 1500 Vol 1 Rev 3
variant (C.F.D.)	In fault tolerance, a version of a program resulting from the application of software diversity.	ISO/IEC 24765:2017
	One of two or more code symbols having the same plain text equivalent.	
	C.F.D. Rationale: Limited applicability	
verification	A test of a system to prove that it meets all its specified requirements at a particular stage of its development.	ISO/IEC 24765:2017 (adapted)
	A process whose purpose is to provide objective evidence that a system or system element fulfills its specified requirements and characteristics.	ISO/IEC 15288:2015
	Note: Methods of performing verification action generally include inspection, analysis, demonstration, or test.	
	Contrast with *validation*	
verifier	An entity that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.	NIST SP 800-63-3
virtual private network (VPN)	Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.	
	Restricted-use logical computer network that is constructed from the system resources of a physical network by using encryption and/or by tunneling links of the virtual network across the real network.	IETF RFC 4949 Ver 2 (adapted)

virus	Type of malicious software that propagates itself by modifying other programs to include a possibly changed copy of itself and that is executed when the infected program is invoked. Note: A virus often causes damage and may be triggered by some event such as the occurrence of a predetermined date	ISO/IEC 2382:2015
	See *malicious code* and *malicious logic*.	
voice over internet protocol (VoIP)	A group of technologies used to provide voice/video/collaboration communications over a data network using internet protocols.	CNSSI No. 5000 (adapted)
vulnerability	A known weakness in a system, system security procedures, internal controls, or implementation by which an actor or event may intentionally exploit or accidentally trigger the weakness to access, modify, or disrupt normal operations of a system—resulting in a security incident or a violation of the system's security policy.	
	Characteristic of design, location, security posture, operation, or any combination thereof, that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation.	DHS Lexicon
	See *weakness.*	
volatility	The potential, tendency, or susceptibility of data, systems, system components, or entities to change over time, change in response to environmental input, or change without a known cause.	
vulnerability analysis	See *vulnerability assessment*.	
vulnerability assessment (VA)	Product or process of identifying attributes that render an entity, asset, system, network, or geographic area susceptible or exposed to threats.	DHS Lexicon (adapted)
	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.	
	See *weakness.*	

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.	NIST SP 800-34 Rev. 1
watering hole attack	A security exploit where the attacker infects websites that are frequently visited by members of the group being targeted, with a goal of infecting a computer used by one of the targeted group when they visit the infected website.	NIST SP 800-150 (adapted)
weakly bound credentials	Credentials that are bound to a subscriber in a manner than can be modified without invalidating the credential.	NIST SP 800-63-3
weakness	An attribute or characteristic that may, under known or unknown conditions, render an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard. See *vulnerability.*	DHS Lexicon (adapted from the definition for vulnerability)
white box testing	A method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e., black box testing). Also known as: "clear box testing", "comprehensive testing", "glass box testing", "transparent box testing", and "structural testing". Contrast with *black box testing.*	NIST SP 800-192
whitelist	A list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorized to be present or active on a system according to a well-defined baseline. Note: Whitelist is also known as "allow list/allowlist."	NIST SP 800-167
	See *clean word list*. Compare with *blacklist*, *graylist*.	
whitelisting	A process used to identify software programs that are authorized to execute on a system or authorized Universal Resource Locators (URL)/websites. Note: Whitelisting is also known as "allow listing/allowlisting." Compare with *blacklisting*.	NIST SP 800-171 Rev. 2

white team	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.	
	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.	
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 and stop unauthorized or suspicious wireless transmissions or activities.	DoDI 8420.01
wireless access point (WAP)	Device or piece of equipment that allows wireless devices to connect to a wired network.	ISO/IEC 27033-6:2016
wireless application protocol (WAP)	A standard that defines the way in which Internet communications and other advanced services are provided on wireless mobile devices.	NIST SP 800-101 Rev. 1
wireless technology	Technology that permits the transfer of information between separated points without physical connection.	NIST SP 800-171 Rev. 2 (adapted)
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.	CNSSI No. 4005
work factor	An estimate of the effort or time needed by a potential perpetrator with specified expertise and resources to overcome a protective measure.	**NCSC-TG-004*

worm	Self-contained program that can propagate itself through data processing systems or computer networks. Note: Worms are often designed to use up available resources such as storage space or processing time.	ISO/IEC 2382:2015
	See *malicious code* and *malicious logic*.	
X.509 public-key certificate	A digital certificate containing a public key for an entity and a unique name for that entity together with some other information that is rendered un-forgeable by the digital signature of the certification authority that issued the certificate, which is encoded in the format defined in the ISO/ITU-T X.509 standard.	NIST SP 800-57 Part 1 Rev. 5
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.	**FIPS 140-2*
zeroize	To remove or eliminate the key from cryptographic equipment or a fill device.	CNSSI No. 4005
zero trust	An evolving set of CS paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.	NIST SP 800-207
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
AAL	Authenticator Assurance Level
ABAC	Attribute Based Access Control
ACCM	Alternative Compensatory Control Measures
ACD	Active Cyber Defense
ACL	Access Control List
AES	Advanced Encryption Standard
AKP	Advanced Key Processor
ALC	Accounting Legend Code
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
AP	Assured Pipeline
APT	Advanced Persistent Threat
ARF	Asset Reporting Format
ASCII	American Standard Code for Information Interchange
ASIC	Application-Specific Integrated Circuit
AS&W	Attack Sensing and Warning
AT	Anti-tamper/Anti-tampering
ATO	Authorization to Operate
BoE	Body of Evidence
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BMA	Business Mission Area
CA	Certificate/Certification Authority

CAC	Common Access Card
CALD	Central Audit and Logging Daemon
CAS	Certification Authority System
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CCB	1. Configuration Control Board 2. Change Control Board
CCE	Common Configuration Enumeration
CCEP	Commercial COMSEC Evaluation Program
CCEVS	Common Criteria Evaluation and Validation Scheme
CCI	1. Controlled Cryptographic Item(s) 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
CIRC	1. Computer Incident Response Center 2. Computer Incident Response Capability
CIRT	1. Cyber Incident Response Team 2. Computer Incident Response Team

CISO	Chief Information Security Officer
CJD	Central Journal Daemon
CKG	Cooperative Key Generation
CKL	Compromised Key List
CKMS	Cryptographic Key Management System
CM2	Cryptographic Modernization 2
CMCS	COMSEC Material Control System
CMDAUTH	Command Authority
CMI	Cryptographic Modernization Initiative
CMVP	Cryptographic Module Validation Program
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CNSA	Commercial National Security Algorithm
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
COMSEC	Communications Security
CONAUTH	Controlling Authority
CONOP	Concept of Operations
COOP	Continuity of Operations Plan

COR	Central Office of Record (COMSEC)
COTS	Commercial off-the-shelf
CP	Certificate Policy
CPE	Common Platform Enumeration
CPS	Certification Practice Statement
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
CSP	1. Common Services Provider 2. Credential Service Provider
CSRF	Cross-site Request Forgery
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
D/A	Department/Agency
D/S	Directory Service

DC3	Defense Cyber Crime Center
DCA	Defense Critical Assets
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
DEA	Data Encryption Algorithm
DEMIL	Demilitarization
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DIMA	DoD portion of the Intelligence Mission Area
DISN	Defense Information System Network
DMZ	Demilitarized Zone
DN	Distinguished Name
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
DRBG	Deterministic Random Bit Generator
DRP	Disaster Recovery Plan
DSOC	DoD Strategy for Operating in Cyberspace
DTD	Data Transfer Device
EA	Enterprise Architecture
EAP	Emergency Action Plan

ECDS	Enterprise Cross Domain Service(s)
ECDSP	Enterprise Cross Domain Service Provider
ECG	Enduring Constitutional Government
ECU	End Cryptographic Unit
EDE-CIS	Ethernet Data Encryption Cryptographic Interoperability Specification
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
FAL	Federation Assurance Level
FAR	False Accept Rate
FBCA	Federal Bridge Certification Authority
FEA	Federal Enterprise Architecture
FICAM	Federated Identity, Credential and Access Management
FIPP	Fair Information Practice Principle
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOE	Filter Orchestration Engine
FOSS	Free and Open Source Software
FRR	False Reject Rate
GOTS	Government-off-the-Shelf
GP-ECDS	General Purpose Enterprise Cross Domain Service
GP-ECDSP	General Purpose Enterprise Cross Domain Service Provider
GSS	General Support System

HAIPE	High Assurance Internet Protocol Encryptor
HAIPE-IS	High Assurance Internet Protocol Encryptor Interoperability Specification
H-ISAC	Health Information Sharing and Analysis Center
HMAC	Hash- Based Message Authentication Code
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
I&A	Identification and Authentication
IAB	Internet Architecture Board
IAL	Identity Assurance Level
IATT	Interim Authorization to Test
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
IC ITE	Intelligence Community Information Technology Enterprise
ICS	1. Intelligence Community Standard 2. Industrial Control System
ICT	Information and Communications Technology
ICTS	Intelligence Community Technical Specification
IdP	Identity Provider
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IDT	Integrated Design Team
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
INFOSEC	Information Systems Security

IO	Information Operations
IP	Internet Protocol
IPC	Inter-Process Communications
IPS	Intrusion Prevention System
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
ISR	Intelligence, Surveillance, and Reconnaissance
ISSE	Information Systems Security Engineer
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
ITU	International Telecommunication Union
IVA	Independent Validation Authority
IV&V	Independent Verification and Validation
JIE	Joint Information Environment
JP	Joint Publication
JSON	JavaScript Object Notation
KDC	Key Distribution Center
KEK	Key Encryption Key
KLV	Key-Length-Value
KME	Key Management Entity

KMI	Key Management Infrastructure
KMID	Key Management Identification Number
KMS	Key Management System
KOA	KMI Operating Account
KOAM	KMI Operating Account Manager
KP	Key Processor
KPC	KMI Protected Channel
LAN	Local Area Network
LCMS	Local COMSEC Management Software
LEF-CIS	Link Encryption Family Cryptographic Interoperability Specification
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
LSI	Large Scale Integration
MAC	1. Mandatory Access Control 2. Message Authentication Code
MACsec	Media Access Control Security
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
MS-ECDS	Mission-Specific Enterprise Cross Domain Service
MS-ECDSP	Mission-Specific Enterprise Cross Domain Service Provider
MSK	Message Signature Key
MSL	Multiple Security Levels
NAG	New Architecture Group
NASA	National Aeronautics and Space Administration
NCIRS	National COMSEC Incident Reporting System
NGE	Next Generation Encryption
NIAP	National Information Assurance Partnership
NII	National Information Infrastructure
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Internal Report
NLZ	No-Lone Zone
NPE	Non-Person Entity
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSEP	National Security Emergency Preparedness
NSI	National Security Information
NSPM	National Security Presidential Memorandum
NSS	National Security System
NSTISSAM	National Security Telecommunications and Information Systems Security Advisory/Information Memorandum
NSTISSD	National Security Telecommunications and Information Systems Security Directive
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NTISSI	National Telecommunications and Information Systems Security Instruction
NVD	National Vulnerability Database

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
OTNK	Over-the-Network Keying
OVAL	Open Vulnerability Assessment Language
PA	Protocol Adapter
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
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
P.L.	Public Law
PLC	Programmable Logic Controller
POA&M	Plan of Action and Milestones
POSIX	Portable Operating System Interface for Unix
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
RAR	Risk Assessment Report
RAdAC	Risk Adaptable Access Control
RBAC	Role Based Access Control
RBG	Random Bit Generator
RD	Restricted Data
RF	Radio Frequency
RMF	Risk Management Framework
RMP	Risk Mitigation Plan
RNG	Random Number Generator
ROM	Read-Only Memory
RP	Relying Party

SA	1. System Administrator 2. Situational Awareness 3. Secure Association
SAISO	Senior Agency Information Security Officer
SAK	Secure Association Key
SAML	Security Assertion Markup Language
SAOP	Senior Agency Official for Privacy
SAP	Special Access Program
SAPF	Special Access Program Facility
SAR	Security Assessment Report
SC	Secure Channel
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
SDS	Secure DTD2000 System
SED	1. Self-Encrypting Devices 2. Self-Encrypting Drives
SFA	Security Fault Analysis
SHA	Secure Hash Algorithm
SISO	Senior Information Security Officer
SKL	Simple Key Loader
SLA	Service Level Agreement
S/MIME	Secure/Multipurpose Internet Mail Extensions
SML	Strength of Mechanism
SMTP	Simple Mail Transfer Protocol

SP	Special Publication
SPK	Single Point Key(ing)
SRG	Security Requirements Guide
SRTM	Security Requirements Traceability Matrix
SSA	Shared Situational Awareness
SSE	Systems Security Engineering
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
STU	Secure Telephone Unit
SwA	Software Assurance
SWID	Software Identification
TA	1. Traffic Analysis 2. Trusted Agent
TADIL-J	Tactical Digital Information Link-J
TC	Technical Community
TCB	Trusted Computing Base
TCP	Transmission Control 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
TrKEK	Transfer Key Encryption Key
TRM	Technical Reference Model
TSCM	Technical Surveillance Countermeasures
TSEC	Telecommunications Security
UAS	User Applications Software
UCDSMO	Unified Cross Domain Services Management Office
UDP	User Datagram Protocol
UID	Unique Identifier
URL	Universal Resource Locators
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
U.S.C.	United States Code
U.S.G.	United States Government
USMTF	United States Message Text Format
UUID	Universally Unique Identifier
VA	Vulnerability Assessment
VMF	Variable Message Format
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	1. Wireless Access Point 2. Wireless Application Protocol
WIDS	Wireless Intrusion Detection System
WLAN	Wireless Local Area Network
WMA	Warfighting Mission Area

WPA2	Wi-Fi Protected Access - 2
XACML	eXtensible Access Control Markup Language
XCCDF	eXtensible Configuration Checklist Description Format
XML	Extensible Markup Language
XSS	Cross-site Scripting

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. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2001.
3. Chairman of the Joint Chiefs of Staff Instruction 6211.02D, *Defense Information Systems Network (DISN) Responsibilities*, current as of August 2015.
4. Committee on National Security Systems Advisory Memoranda (CNSSAM) TEMPEST/1-13, *RED/BLACK Installation Guidance*, January 2014.
5. Committee on National Security Systems Advisory Memoranda (CNSSAM) Information Assurance (IA)/01-12, *NSA-Approved Commercial Solution Guidance*, June 2012.
6. Committee on National Security Systems Directive (CNSSD) No. 504, *Directive on Protecting National Security Systems from Insider Threat*, September 2016.
7. Committee on National Security Systems Directive (CNSSD) No. 505, *Supply Chain Risk Management*, August 2017.
8. Committee on National Security Systems Directive (CNSSD) No. 507, *National Directive for Identity, Credential, and Access Management Capabilities on the United States Federal Secret Fabric*, July 2020.
9. Committee on National Security Systems Instruction (CNSSI) No. 1011, *Implementing Host-Based Security Capabilities on National Security Systems*, July 2013.
10. Committee on National Security Systems Instruction (CNSSI) No. 1012, *Instruction for Network Mapping of National Security Systems (NSS)*, July 2013.
11. 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.
12. Committee on National Security Systems Instruction (CNSSI) No. 1015, *Enterprise Audit Management Instruction for National Security Systems (NSS)*, September 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 2017.
16. Committee on National Security Systems Instruction (CNSSI) No. 1254, *Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems*, August 2016.
17. Committee on National Security Systems Instruction (CNSSI) No. 1300, *Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy, Under CNSS Policy No. 25*, December 2014.
18. Committee on National Security Systems Instruction (CNSSI) No. 4000, *Maintenance of Communications Security (COMSEC) Equipment*, October 2012.
19. Committee on National Security Systems Instruction (CNSSI) No. 4001, *Controlled Cryptographic Items*, May 2013.
20. Committee on National Security Systems Instruction (CNSSI) No. 4003, *Reporting and Evaluating Communications Security (COMSEC) Incidents*, June 2016.
21. Committee on National Security Systems Instruction (CNSSI) No. 4004.1, *Destruction and Emergency Protection Procedures for COMSEC and Classified Material*, January 2008.
22. Committee on National Security Systems Instruction (CNSSI) No. 4005, *Safeguarding COMSEC Facilities and Materials*, August 2011.
23. Committee on National Security Systems Instruction (CNSSI) No. 4006, *Controlling Authorities for Traditional COMSEC Keying Material*, December 2012.
24. Committee on National Security Systems Instruction (CNSSI) No. 4031, *Cryptographic High Value Products*, August 2019.
25. Committee on National Security Systems Instruction (CNSSI) No. 4032, *Management and Use of Secure Data Network Systems*, June 2012.
26. Committee on National Security Systems Instruction (CNSSI) No. 4033, *Nomenclature for Communications Security Material*, November 2012.
27. Committee on National Security Systems Instruction (CNSSI) No. 5000, *Voice over Internet Protocol (VoIP) Telephony*, October 2016.
28. Committee on National Security Systems Instruction (CNSSI) No. 7003, *Protected Distribution Systems*, September 2015.
29. 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.

30. Committee on National Security Systems Policy (CNSSP) No. 11, *Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, June 2013.
31. Committee on National Security Systems Policy (CNSSP) No. 15, *Use of Public Standards for Secure Information Sharing*, October 2016.
32. Committee on National Security Systems Policy (CNSSP) No. 19, *National Policy Governing the Use of High Assurance Internet Protocol Encryptor (HAIPE)*, June 2013.
33. Committee on National Security Systems Policy (CNSSP) No. 24, *Policy on Assured Information Sharing (AIS) for National Security Systems (NSS)*, May 2010.
34. Common Criteria Maintenance Board (CCMB)-2017-04-001, *Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 5, April 2017.
35. DAMA International, *Guide to the Data Management Body of Knowledge (DAMA-DMBOK2)*, 2nd Edition, 2017.
36. Defense Acquisition University Glossary, https://www.dau.edu/glossary/Pages/Glossary.aspx, accessed September 2019.
37. Defense Information Systems Agency Risk Management Executive, *Defense Information Systems Network (DISN) Connection Process Guide (CPG)*, Version 5.1, September 2016.
38. Department of Defense 2016 Major Automated Information System Annual Report, *Key Management Infrastructure Increment 2 (KMI Inc 2)*, 2016.
39. Department of Defense Dictionary of Military and Associated Terms, August 2021, as amended [formerly known as Department of Defense Joint Publication 1-02].
40. Department of Defense Directive (DoDD) 3020.26, *DoD Continuity Policy*, February 2018.
41. Department of Defense Directive (DoDD) 3020.40, *Mission Assurance (MA)*, November 2016, Change 1, September 11, 2018.
42. Department of Defense Directive (DoDD) 5205.02E, *DoD Operations Security (OPSEC) Program*, June 2012, Incorporating Change 2, August 20, 2020.
43. Department of Defense Directive (DoDD) 5505.13E, *DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)*, March 2010, Incorporating Change 1, July 27, 2017.
44. Department of Defense Directive (DoDD) 8140.01, *Cyberspace Workforce Management*, October 2020.
45. Department of Defense Instruction (DoDI) 1000.13, *Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*, January 2014, Incorporating Change 1, December 14, 2017.

46. Department of Defense Instruction (DoDI) 3020.45, *Mission Assurance (MA) Construct*, August 2018.
47. Department of Defense Instruction (DoDI) 4000.19, *Support Agreements*, December 2020.
48. Department of Defense Instruction (DoDI) 5200.39, *Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)*, May 2015, Incorporating Change 3, October 1, 2020.
49. Department of Defense Instruction (DoDI) 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, November 2012, Incorporating Change 3, October 15, 2018.
50. Department of Defense Instruction (DoDI) 5230.09, *Clearance of DoD Information for Public Release*, January 2019.
51. Department of Defense Instruction (DoDI) 5240.05, *Technical Surveillance Countermeasures (TSCM)*, April 2014, Incorporating Change 2, August 27, 2020.
52. Department of Defense Instruction (DoDI) 8115.02, *Information Technology Portfolio Management Implementation*, October 2006.
53. Department of Defense Instruction (DoDI) 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies*, November 2017.
54. Department of Defense Instruction (DoDI) 8500.01, *Cybersecurity*, March 2014, Incorporating Change 1, October 7, 2019.
55. Department of Defense Instruction (DoDI) 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, March 2014, Incorporating Change 3, December 29, 2020.
56. Department of Defense Instruction (DoDI) 8540.01, *Cross Domain (CD) Policy*, August 2017, Incorporating Change 1, August 28, 2017.
57. Department of Defense Joint Information Environment (JIE) Network Normalization and Transport (NTT) Integrated Design Team (IDT) Wide Area Network (WAN) Solution Architecture (nd)
58. Department of Defense Joint Publication (JP) 2-0, Joint Intelligence, October 2013.
59. Department of Defense Joint Publication (JP) 3-0, *Joint Operations*, January 2017, Incorporating Change 1, October 22, 2018.
60. Department of Defense Joint Publication (JP) 3-12, *Cyberspace Operations*, June 2018.
61. Department of Defense Joint Publication (JP) 3-13, *Information Operations*, November 2012, Incorporating Change 1, November 20, 2014.
62. Department of Defense Joint Publication (JP) 3-27, *Homeland Defense*, April 2018.
63. Department of Defense Joint Publication (JP) 6-0, *Joint Communications System*, June 2015, Incorporating Change 1, October 4, 2019.

64. Department of Defense Manual (DoDM) 4140.01, Volume 2, *DoD Supply Chain Materiel Management Procedures: Demand and Supply Planning*, November 2018.
65. Department of Defense Manual (DoDM) 4160.21, Volume 1, *Defense Materiel Disposition: Disposal Guidance and Procedures*, 22 October 2015, Incorporating Change 3, October 2, 2019.
66. Department of Defense Manual (DoDM) 4160.28, Volume 1, *Defense Demilitarization: Program Administration*, 7 June 2011, Incorporating Change 3, July 15, 2019.
67. Department of Defense Manual (DoDM) 5205.07, Volume 4, *Special Access Program (SAP) Security Manual: Marking*, October 2013, Incorporating Change 2, September 8, 2020.
68. *Department of Defense Standard (DoD STD) 5200.28, *Department of Defense Trusted Computer System Evaluation Criteria, [Orange Book],* December 1985. **Superseded by DoDI 8500.01, March 2014.*
69. Department of Defense Strategy for Operating in Cyberspace (DSOC), July 2011.
70. Department of Homeland Security Office of Inspector General (OIG) 11-121, *Management Advisory Report on Cybersecurity*, September 2011.
71. Department of Homeland Security, *Information Technology Sector Baseline Risk Assessment*, August 2009.
72. Department of Homeland Security, *Instruction Manual 262-12-001-01, DHS Lexicon Terms and Definitions, 2017 Edition - Revision 2*, October 2017.
73. Encyclopedia Britannica, https://www.britannica.com, September 2021.
74. Executive Order (E.O.) 12333, as amended, *United States Intelligence Activities*, December 1981.
75. Executive Order (E.O.) 13526, *Classified National Security Information,* December 2009.
76. Executive Order (E.O.) 13556, *Controlled Unclassified Information*, November 2010.
77. *Federal Identity, Credential, and Access Management (FICAM) Architecture*: Services Framework, https://arch.idmanagement.gov/services/, page accessed July 2020.
78. *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, Version 2.0, December 2011.
79. Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001.
80. Federal Information Processing Standard (FIPS) Publication 180-4, *Secure Hash Standard (SHS)*, August 2015.
81. Federal Information Processing Standard (FIPS) Publication 197, *Advanced Encryption Standard (AES)*, November 2001.
82. Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

83. Federal Information Processing Standard (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
84. Federal Information Processing Standard (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013.
85. Health Information Sharing and Analysis Center (H-ISAC), *Blended Threats White Paper*, December 2019.
86. Information Sharing Architecture (ISA) Shared Situational Awareness (SSA), *Requirements Document*, version 2.1, October 2013.
87. Intelligence Community Directive (ICD) No. 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information*, June 2013.
88. Intelligence Community Standard (ICS) 500-30, *Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources*, April 2014.
89. Intelligence Community Standard (ICS) 502-01, *Intelligence Community Computer Incident Response and Computer Network Defense*, December 2013.
90. Intelligence Community Standard (ICS) 700-1, *Glossary of Security Terms, Definitions, and Acronyms*, April 2008.
91. Intelligence Community Technical Specification (ICTS), Unified Identity Attribute Set (UIAS) v2.1, *IC Enterprise Attribute Exchange between IC Attribute Services Unified Identity Attribute Set*, September 2019.
92. International Organization for Standardization (ISO) 3676:2012, *Packaging - Complete, filled transport packages and unit loads - Unit load dimensions*, 2012.
93. International Organization for Standardization (ISO) 10377:2013, *Consumer product safety - Guidelines for suppliers*, 2013.
94. International Organization for Standardization (ISO) 15638-1:2012, *Intelligent transport systems - Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) - Part 1: Framework and architecture*, 2012.
95. International Organization for Standardization (ISO) 30400:2016, *Human resource management - Vocabulary*, 2016.
96. International Organization for Standardization (ISO) 30401:2018, *Knowledge management systems -Requirements*, 2018.
97. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 2382:2015, *Information Technology - Vocabulary*, 2015.

98. 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.
99. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 14908-4:2012, *Information technology - Control network protocol - Part 4: IP communication*, 2012.
100. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15288:2015, *Systems and software engineering - System life cycle processes*, 2015.
101. 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.
102. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 18033-1:2021, *Information Security - Encryption algorithms - Part 1: General*, 2021.
103. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 19770-2:2015, *Information technology - IT asset management -- Part 2: Software identification tag*, 2017.
104. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 19790:2012, *Information technology -- Security techniques -- Security requirements for cryptographic modules*, 2012.
105. 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.
106. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 21371:2018, *Traditional Chinese medicine - Labelling requirements of products intended for oral or topical use*, 2018.
107. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 24765:2017, *Systems and software engineering - Vocabulary*, 2017.
108. 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.
109. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) ISO/IEC 27033-6:2016, *Information technology -Security techniques - Network Security - Part 6: Securing wireless IP network access*, 2016.

110. International Telecommunication Union (ITU) Recommendation X.500, *Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services*, October 2019.
111. International Telecommunication Union (ITU) Recommendation X.509, *Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*, October 2016.
112. Internet Engineering Task Force (IETF) Request for Comments (RFC) 4301, *Security Architecture for the Internet Protocol*, December 2005.
113. Internet Engineering Task Force (IETF) Request for Comments (RFC) 4949 Version 2, *Internet Security Glossary*, August 2007.
114. Internet Engineering Task Force (IETF) Request for Comments (RFC) 5907, *Definitions of Managed Objects for Network Time Protocol Version 4*, June 2010.
115. Internet Engineering Task Force (IETF) Request for Comments (RFC) 5920, *Security Framework for MPLS and GMPLS Networks*, July 2010.
116. Internet Engineering Task Force (IETF) Request for Comments (RFC) 8446, *The Transport Layer Security (TLS) Protocol*, Version 1.3, August 2018.
117. MITRE, *Common Vulnerabilities and Exposures (CVE)*, http://cve.mitre.org/, page accessed July 2020.
118. MITRE, *Common Weakness Enumeration (CWE): Frequently Asked Questions*, Paragraph A1, https://cwe.mitre.org/about/faq.html, page accessed July 2019.
119. National Aeronautics and Space Administration (NASA) Technical Standard (NASA-STD) 8739.8 w/Change 1, *Software Assurance Standard*, July 2004.
120. *National Computer Security Center (NCSC) Technical Guide 004 (NCSC-TG-004), *Glossary of Computer Security Terms, [Aqua Book]*, October 1988. **Superseded by the Common Criteria for Information Technology Security Evaluation, 2005.*
121. *National Computer Security Center (NCSC) Technical Guide 025 (NCSC-TG-025), *A Guide to Understanding Data Remanence in Automated Information Systems, [Forest Green Book]*, September 1991.
122. National Information Assurance Partnership Technical Decision 0301, *Updates to Administrator Management and Biometric Authentication*, April 2018.
123. National Institute of Standards and Technology (NIST) Handbook 150, *National Voluntary Laboratory Accreditation Program: Procedures and General Requirements*, February 2018.
124. National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) Bulletin, *The National Vulnerability Database (NVD): Overview*, December 2013.

125. National Institute of Standards and Technology (NIST) Interagency Report (IR) 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*, October 2012.
126. National Institute of Standards and Technology (NIST) Interagency Report (IR) 7657, *A Report on the Privilege (Access) Management Workshop*, March 2010.
127. National Institute of Standards and Technology (NIST) Internal Report (IR) 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, January 2017.
128. National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP), https://www.nist.gov/nvlap/accreditation-vs-certification, accessed June 2019.
129. National Institute of Standards and Technology (NIST) Privacy Framework, *A Tool for Improving Privacy Through Enterprise Risk Management*, Version 1.0, January 2020.
130. *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12 Rev. 1, *An Introduction to Information Security*, June 2017. **Withdrawn*
131. 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.
132. *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. ***Superseded by NIST SP 800-160 Vol.1*
133. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-28 Version 2, *Guidelines on Active Content and Mobile Code*, March 2008.
134. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Rev. 1, *Guide for Conducting Risk Assessments*, September 2012.
135. National Institute of Standards and Technology (NIST) Special Publication (SP), 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001.
136. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.
137. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 2018.
138. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.
139. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-41 Rev. 1, *Guidelines on Firewalls and Firewall Policy*, September 2009.

140. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-45 Version 2, *Guidelines on Electronic Mail Security*, February 2007.
141. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.
142. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-49, *Federal S/MIME V3 Client Profile*, November 2002.
143. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, December 2020.
144. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, December 2014.
145. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-56B Rev. 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*, March 2019.
146. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-57 Part 1 Rev. 5, *Recommendation for Key Management: Part 1 - General*, May 2020.
147. 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.
148. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 Volume 1 Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.
149. *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev. 1, *Computer Security Incident Handling Guide*, March 2008. **Superseded by NIST SP 800-61 Rev. 2*
150. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev. 2, *Computer Security Incident Handling Guide*, August 2012.
151. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, *Digital Identity Guidelines*, March 2020.
152. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-67 Rev. 2 *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, November 2017.
153. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-72, *Guidelines on PDA Forensics*, November 2004.
154. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 Rev. 2, *Guide to Industrial Control Systems (ICS) Security*, May 2015.

155. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88 Rev. 1, *Guidelines for Media Sanitization*, December 2014.
156. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*, November 2006.
157. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-94, *Guide to Intrusion Detection and Prevention Systems* (*IDPS*), February 2007.
158. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-101 Rev. 1, *Guidelines on Mobile Device Forensics*, May 2014.
159. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-107 Rev. 1, *Recommendation for Applications Using Approved Hash Algorithms*, August 2012.
160. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-126 Rev. 3, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3*, February 2018.
161. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, October 2019.
162. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011.
163. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing: Recommendations from the National Institute of Standards and Technology*, September 2011.
164. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-150, *Guide to Cyber Threat Information Sharing*, October 2016.
165. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160 Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, 21 March 2018.
166. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015.
167. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, March 2018.
168. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-163 Rev. 1, *Vetting the Security of Mobile Applications*, April 2019.
169. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-167, *Guide to Application Whitelisting*, October 2015.

170. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Rev. 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, February 2020.
171. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-175A, *Guidelines for Using Cryptographic Standards in the Federal Government: Directives, Mandates, and Policies*, August 2016.
172. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-192, *Verification and Test Methods for Access Control Policies/Models*, June 2017.
173. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, *Zero Trust Architecture*, August 2020.
174. National Institute of Standards and Technology (NIST) Special Publication (SP) 1500 Volume 1 Revision 3, *NIST Big Data Interoperability Framework: Volume 1, Definitions*, October 2019.
175. National Security Agency (NSA), *Cross Domain Solution (CDS) Design and Implementation Requirements – 2018 Raise the Bar (RTB) Baseline Release*, 2018.
176. 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.
177. National Security Agency/Central Security Service (NSA/CSS) Policy 1-50, *Program Performance Management*, October 2020.
178. National Security Agency/Central Security Service (NSA/CSS) Policy 3-3, *Management of the Production of Nuclear Command and Control Information Assurance Material*, August 2020.
179. National Security Agency/Central Security Service (NSA/CSS) Policy 3-4, *Acquisition and Integration of Cybersecurity and Cybersecurity-Enabled Information Technology (IT) Products*, October 2019.
180. National Security Agency/Central Security Service (NSA/CSS) Policy 3-12, *NSA/CSS Use of Protected Distribution Systems*, December 2019.
181. 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.
182. National Security Agency/Central Security Service (NSA/CSS) Policy 6-10, *Control and Management of Software*, June 2018.
183. National Security Agency/Central Security Service (NSA/CSS) Policy 11-1, *Information Sharing*, October 2020.
184. National Security Agency/Central Security Service (NSA/CSS) Policy 11-11, *NSA/CSS Cybersecurity Signatures and Indicators of Malicious Cyber Activity*, December 2019.

185. National Security Agency/Central Security Service (NSA/CSS) Policy Manual Number 9-12, *NSA/CSS Storage Device Sanitization Manual*, December 2017.
186. National Security Agency, *Information Assurance Security Requirements Directive (IASRD-001-2016)*, July 2016.
187. National Security Agency, *Information Assurance Technical Framework (IATF)*, Release 3.1, Appendix B, September 2002.
188. National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23, *Cybersecurity Policy*, January 2008.
189. National Security Presidential Memorandum/NSPM-13, *United States Cyber Operations Policy*, August 2018.
190. National Security Telecommunications and Information Systems Security Directive (NSTISSD) 501, *National Security Program for Information Systems Security (INFOSEC) Professionals*, November 1992.
191. National Security Telecommunications and Information Systems Security Directive (NSTISSD) 600, *Communications Security Monitoring*, April 1990.
192. 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.
193. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7002 (TEMPEST), *TEMPEST Glossary*, March 1995.
194. OASIS Open, *XACML Version 3.0 Plus Errata 01*, http://docs.oasis-open.org/xacml/3.0/errata01/os/xacml-3.0-core-spec-errata01-os-complete.html#_Toc489959470, July 2017, page accessed January 2021.
195. Office of the Director of National Intelligence (ODNI), *About the ISE*, https://www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ise/about-the-ise, page accessed January 2021.
196. Office of the Director of National Intelligence (ODNI), *Intelligence Community (IC) Data Management Lexicon (DML)*, January 2020.
197. Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, July 2016.
198. Office of Management and Budget (OMB) Memorandum 2-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.
199. Office of Management and Budget (OMB) Memorandum 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 2017.

200. Presidential Policy Directive (PPD)-21, *Critical Infrastructure Security and Resilience*, February 2013.
201. Presidential Policy Directive (PPD)-41, *United States Cyber Incident Coordination*, July 2016.
202. Public Law 105-277 [H.R. 4328], Title XVII, *Government Paperwork Elimination Act, Section 1710*, 1998.
203. 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.
204. Public Law 113-283, *Federal Information Security Modernization Act (FISMA) of 2014*, December 2014.
205. Public Law 115-232, *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, August 2018.
206. SearchSecurity, *Link Encryption*, https://searchsecurity.techtarget.com/definition/link-encryption, page accessed July 2020.
207. United States Department of Commerce (USDC), *Defense Industrial Base Assessment: Counterfeit Electronics*, January 2010.
208. United States Government Accountability Office (USGAO), GAO-12-137, *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements*, October 2011.
209. World Intellectual Property Organization (WIPO), *Understanding Copyright and Related Rights*, 2016.
210. 6 Code of Federal Regulations (CFR) 5.41, *Purpose and Scope; definitions*, September 2021.
211. 10 Code of Federal Regulations (CFR) 709.2, *Definitions*, May 2021.
212. 22 Code of Federal Regulations (CFR) 120.15, *U.S. Person*, January 2021.
213. 32 Code of Federal Regulations (CFR) Part 2002.4, *Controlled Unclassified Information - Definitions*, January 2021.
214. 32 Code of Federal Regulations (CFR) Part 2004.4, *Definitions that apply to this part*, January 2021.
215. 47 Code of Federal Regulations (CFR) Part 64 Appendix A, *Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NSEP)*, January 2021.
216. 5 United States Code (U.S.C.) Sec. 552a, *Privacy Act of 1974*, April 2021.
217. 40 United States Code (U.S.C.) Sec. 11101, *Definitions*, January 2021.
218. 40 United States Code (U.S.C.) Sec. 11315, *Agency Chief Information Officer*, January 2021.
219. 40 United States Code (U.S.C.) Sec. 11331, *Responsibilities for Federal information systems standards*, January 2021.
220. 41 United States Code (U.S.C.) Sec. 133, *Definitions*, January 2021.

221. 44 United States Code (U.S.C.) Sec. 3502, *Definitions*, January 2021.
222. 44 United States Code (U.S.C.) Sec. 3552, *Definitions*, January 2021.
223. 50 United States Code (U.S.C.) Sec. 1801, *Definitions*, January 2021.
224. 50 United States Code (U.S.C.) Sec. 3003, *Definitions*, January 2021.