The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Practices

INFORMATION SECURITY GLOSSARY OF TERMS

DRAFT RECOMMENDED PRACTICE

CCSDS 350.8-P-1.1

PINK BOOK

August 2018

The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Practices

INFORMATION SECURITY GLOSSARY OF TERMS

DRAFT RECOMMENDED PRACTICE

CCSDS 350.8-P-1.1

PINK BOOK

August 2018

AUTHORITY

Issue:	Pink Book, Issue 1.1
Date:	August 2018
Location:	Not Applicable

(WHEN THIS RECOMMENDED PRACTICE IS FINALIZED, IT WILL CONTAIN THE FOLLOWING STATEMENT OF AUTHORITY:)

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and represents the consensus technical agreement of the participating CCSDS Member Agencies. The procedure for review and authorization of CCSDS documents is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4), and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the e-mail address below.

This document is published and maintained by:

CCSDS Secretariat
National Aeronautics and Space Administration
Washington, DC, USA
E-mail: secretariat@mailman.ccsds.org

STATEMENT OF INTENT

(WHEN THIS RECOMMENDED PRACTICE IS FINALIZED, IT WILL CONTAIN THE FOLLOWING STATEMENT OF INTENT:)

The Consultative Committee for Space Data Systems (CCSDS) is an organization officially established by the management of its members. The Committee meets periodically to address data systems problems that are common to all participants, and to formulate sound technical solutions to these problems. Inasmuch as participation in the CCSDS is completely voluntary, the results of Committee actions are termed **Recommendations** and are not in themselves considered binding on any Agency.

CCSDS Recommendations take two forms: **Recommended Standards** that are prescriptive and are the formal vehicles by which CCSDS Agencies create the standards that specify how elements of their space mission support infrastructure shall operate and interoperate with others; and **Recommended Practices** that are more descriptive in nature and are intended to provide general guidance about how to approach a particular problem associated with space mission support. This **Recommended Practice** is issued by, and represents the consensus of, the CCSDS members. Endorsement of this **Recommended Practice** is entirely voluntary and does not imply a commitment by any Agency or organization to implement its recommendations in a prescriptive sense.

No later than five years from its date of issuance, this **Recommended Practice** will be reviewed by the CCSDS to determine whether it should: (1) remain in effect without change; (2) be changed to reflect the impact of new technologies, new requirements, or new directions; or (3) be retired or canceled.

In those instances when a new version of a **Recommended Practice** is issued, existing CCSDS-related member Practices and implementations are not negated or deemed to be non-CCSDS compatible. It is the responsibility of each member to determine when such Practices or implementations are to be modified. Each member is, however, strongly encouraged to direct planning for its new Practices and implementations towards the later version of the Recommended Practice.

FOREWORD

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommended Practice is therefore subject to CCSDS document management and change control procedures, which are defined in the *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4). Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be sent to the CCSDS Secretariat at the e-mail address indicated on page i.

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People's Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.
- UK Space Agency/United Kingdom.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
- Chinese Academy of Sciences (CAS)/China.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- Electronics and Telecommunications Research Institute (ETRI)/Korea.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- Mohammed Bin Rashid Space Centre (MBRSC)/United Arab Emirates.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- South African National Space Agency (SANSA)/Republic of South Africa.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- Swiss Space Office (SSO)/Switzerland.
- United States Geological Survey (USGS)/USA.

PREFACE

This document is a draft CCSDS Recommended Practice. Its 'Red Book' status indicates that the CCSDS believes the document to be technically mature and has released it for formal review by appropriate technical organizations. As such, its technical contents are not stable, and several iterations of it may occur in response to comments received during the review process.

Implementers are cautioned **not** to fabricate any final equipment in accordance with this document's technical content.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 350.8-G-1	Information Security Glossary of Terms, Informational Report, Issue 1	November 2012	Original issue
CCSDS 350.8-P-1.1	Information Security Glossary of Terms, Draft Recommended Practice, Issue 1.1	August 2018	Current draft update

CONTENTS

1 INTRODUCTION

1.1 PURPOSE

This document is issued to provide a central source of information security terms and their respective definitions. It is intended that this document will be included as a normative reference in all CCSDS security documents and any CCSDS documents referencing information security.

1.2 SCOPE

This document provides a glossary of information security terms which can be used by all CCSDS document authors.

1.3 APPLICABILITY

This document is applicable to all document authors requiring definitions for information security terms. It may be included as a normative reference in any document requiring the definitions of information security terms.

1.4 RATIONALE

In the past, each CCSDS security-related document generated and included its own glossary of information security terms. Often, because different sources of definitions were consulted, the definitions between documents were not consistent. The document-specific generation of such glossaries also consumed valuable resources. In order to minimize resource utilization and to ensure definition consistency, this document has been created for use as a normative reference by CCSDS document authors.

1.5 REFERENCES

The following publications contain provisions which, through reference in this text, constitute provisions of this document. At the time of publication, the editions indicated were valid. All publications are subject to revision, and users of this document are encouraged to investigate the possibility of applying the most recent editions of the publications indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS publications.

[1] *Information Processing Systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture*. International Standard, ISO 7498-2:1989. Geneva: ISO, 1989.

[2] *Information Technology—Security Techniques—Information Security Management Systems—Requirements*. 2nd ed. International Standard, ISO/IEC 27001:2013. Geneva: ISO, 2013.

[3] *Committee on National Security Systems (CNSS) Glossary*. Revised. CNSSI No. 4009. Fort Meade, Maryland: CNSS, April 6, 2015.

[4] *Glossary of Key Information Security Terms*. Rev. 2. Edited by Richard Kissel. NIST IR 7298. Gaithersburg, Maryland: NIST, May 2013.

[5] Elaine Barker. *Recommendation for Key Management—Part 1: General*. Revision 4. National Institute of Standards and Technology Special Publication 800-57. Gaithersburg, Maryland: NIST, January 2016.

[6] *Recommended Security Controls for Federal Information Systems and Organizations*. Rev. 3. National Institute of Standards and Technology Special Publication 800-53. Gaithersburg, Maryland: NIST, August 2009.

[7] *DOD Dictionary of Military and Associated Terms*. Washington, D.C.: U.S. Department of Defense, April 2018.

[8] *Glossary of INFOSEC and INFOSEC Related Terms*. Compiled by Corey D. Schou. Pocatello, Idaho: Idaho State U Simplot Decision Support Center, 1996.

[9] *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*. 5th ed. International Standard, ISO/IEC 27000:2018 . Geneva: ISO, 2018.

[10] S. Kent. *IP Encapsulating Security Payload (ESP)*. RFC 4303. Reston, Virginia: ISOC, December 2005.

[11] *Information Technology—Security Techniques—Encryption Algorithms—Part 4: Stream Ciphers*. 2nd ed. International Standard, ISO/IEC 18033-4:2011. Geneva: ISO, 2011.

[12] *Software Assurance Standard*. w/Change 1. NASA Technical Standard NASA-STD-8739.8. Washington, DC: NASA, July 28, 2004.

2 OVERVIEW

This document is intended to provide a set of information security terms and their definitions for use as a normative reference in CCSDS documents. The intent is to have a single source of information security terms and definitions. This is desirable so that definitions are not duplicated and do not vary across CCSDS documents.

All of the definitions included in this document were acquired from authoritative sources such as ISO/IEC, NIST, and several others which are listed in the normative references. All of the individual definitions are referenced back to their source.

This glossary ensures the consistency of the definitions across CCSDS.

3 GLOSSARY OF INFORMATION SECURITY TERMS

access control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. (Reference [1].)

access control list, ACL: A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object. (Reference [4].)

access control mechanism: Those mechanisms which are used to enforce a policy of limiting access to a resource to only those users who are authorized. (Reference [1].)

accountability: (1) The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. (2) 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. (Reference [4].)

accreditation: Formal declaration by a senior official that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. (Reference [3].)

accreditation authority: Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. (Reference [4].)

active threat: The threat of a deliberate unauthorized change to the state of the system. (Reference [1].)

advanced encryption standard, AES: A symmetric block cipher using cryptographic key sizes of 128, 192, and 256 bits used to encrypt and decrypt data in blocks of 128 bits. (Reference [3].)

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. (Reference [4].)

advanced persistent threats, 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). (Reference [4].)

NOTE – 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. (Reference [4].)

adversary: Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. (Reference [4].)

anti-jam: The measures taken to ensure that transmitted information can be received despite deliberate jamming attempts. (Reference [3].)

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. (Reference [4].)

asymmetric key algorithm: (See *public key cryptographic algorithm*.)

assurance: Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. 'Adequately met' includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass. (Reference [4].)

assured software: Computer application that has been designed, developed, analyzed, and tested using processes, tools, and techniques that establish a level of confidence in it. (Reference [4].)

attack: Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. (Reference [9].)

audit: An 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. (Reference [1].)

audit trail: Data collected and potentially used to facilitate a security audit. (Reference [1].)

authenticate: To verify the identity of a user, user device, or other entity. (Reference [4].)

authentication: The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. (Reference [3].) (See also *peer-entity authentication* and *data origin authentication*.)

authentication code: A cryptographic checksum based on an Approved security function (also known as a Message Authentication Code [MAC]). (Reference [4].)

authentication mechanism: Hardware or software-based mechanisms that forces users, devices, or processes to prove their identity before accessing data on an information system. (Reference [4].)

authenticity: Property that an entity is what it claims to be. (Reference [9].)

authority: Person(s) or established bodies with rights and responsibilities to exert control in an administrative sphere. (Reference [4].)

authorization: The granting of rights, which includes the granting of access based on access rights. (Reference [1].)

availability: The property of being accessible and useable upon demand by an authorized entity. (Reference [3].)

block cipher: A symmetric key cryptographic algorithm that transforms a block of information at a time using a cryptographic key. (Reference [4].)

NOTE – For a block cipher algorithm, the length of the input block is the same as the length of the output block. (Reference [4].)

block cipher algorithm: A family of functions and their inverses that is parameterized by a cryptographic key; the function maps bit strings of a fixed length to bit strings of the same length. (Reference [4].)

bulk encryption: The simultaneous (protocol-transparent) encryption of all channels of a multichannel telecommunications link. (Reference [3].)

certificate: A digitally signed document that binds a public key with an identity. The certificate contains, at a minimum, the identity of the issuing certification authority (CA), the user identification information, and the user's public key. (Reference [3].)

certification: The comprehensive evaluation of the technical and nontechnical security safeguards of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. (Reference [3].)

certificate authority, CA: Trusted entity authorized to create, sign, and issue public key certificates. By digitally signing each certificate issued, the user's identity is certified, and the association of the certified identity with a public key is validated. (Reference [3].)

certification authority: (See *certificate authority*.)

certificate management: Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed. (Reference [4].)

certificate policy, CP: A specialized form of administrative policy tuned to electronic transactions performed during certificate management. (Reference [4].)

NOTE – 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. (Reference [4].)

certificate revocation list, CRL: A list of revoked public key certificates created and digitally signed by a Certification Authority. (Reference [4].)

challenge-response-protocol: An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a secret (often 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. (Reference [4].)

NOTE – 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. (Reference [4].)

cipher: Series of transformations that converts plaintext to ciphertext using the Cipher Key. (Reference [4].)

cipher suite: Negotiated algorithm identifiers. Cipher suites are identified in human-readable form using a pneumonic code. (Reference [4].)

cipher text: Data produced through the use of encipherment. The semantic content of the resulting data is not available. (Reference [1].)

classification: The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made. (Reference [7].)

cloud computing: A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (Reference [4].)

NOTE – Cloud computing allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud). (Reference [4].)

common criteria, CC: A standard (ISO/IEC 15408) providing a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems. (Reference [3].)

common control: A security control that is inherited by one or more organizational information systems. (Reference [4].)

computer cryptography: Use of a crypto-algorithm program by a computer to authenticate or encrypt/decrypt information. (Reference [4].)

computer forensics: The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. (Reference [4].)

computer network attack, CNA: Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (Reference [4].)

computer network defense, CND: Actions taken to defend against unauthorized activity within computer networks. (Reference [4].)

NOTE – CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities. (Reference [4].)

configuration management: (See *configuration control*.)

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. (Reference [3].)

confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (Reference [1].)

countermeasures: Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. (Reference [3].)

covert channel: An unauthorized communication path that manipulates a communications medium in an unexpected, unconventional, or unforeseen way in order to transmit information without detection by anyone other than the entities operating the covert channel. (Reference [4].)

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. (Reference [4].)

credential: An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber. (Reference [4].)

cryptanalysis: Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection. (Reference [5].)

cryptography: The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. (Reference [1].)

cryptographic algorithm: A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output. (Reference [5].)

cryptographic boundary: An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all hardware, software, and/or firmware components of a cryptographic module. (Reference [5].)

cryptographic key: A binary string used as a secret parameter by a cryptographic algorithm. (Reference [4].)

cryptographic module: The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. (Reference [4].)

crypto period: The time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect. (Reference [5].)

cyber attack: An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. (Reference [4].)

cyber incident: Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. (Reference [4].)

cybersecurity: The ability to protect or defend the use of cyberspace from cyber attacks. (Reference [4].)

data integrity: The property that data has not been changed, destroyed, or lost in an unauthorized manner. (Reference [3].)

data origin authentication: The corroboration that the source of data received is as claimed. (Reference [1].)

decipherment: The reversal of a corresponding reversible encipherment. (Reference [1].).

decryption: (See *decipherment*.)

defense-in-depth: Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization. (Reference [3].)

denial of service, DOS: The prevention of authorized access to resources or the delaying of time-critical operations. (Reference [1].)

digital certificate: (See *certificate*.)

digital signature: Data appended to, or a cryptographic transformation (see *cryptography*) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g., by the recipient. (Reference [1].)

digital signature algorithm: Asymmetric algorithms used for digitally signing data. (Reference [4].)

discretionary access control, DAC: An access control policy that is enforced over all subjects and objects in an information system where the policy specifies that a subject that has been granted access to information can do one or more of the following: (i) pass the information to other subjects or objects; (ii) grant its privileges to other subjects; (iii) change security attributes on subjects, objects, information systems, or system components; (iv) choose the security attributes to be associated with newly-created or revised objects; or (v) change the rules governing access control. Mandatory access controls restrict this capability. (Reference [3].)

electronic credentials: Digital documents used in authentication that bind an identity or an attribute to a subscriber's token. (Reference [4].)

embedded cryptographic system: Cryptosystem performing or controlling a function as an integral element of a larger system or subsystem. (Reference [4].)

embedded cryptography: Cryptography engineered into an equipment or system whose basic function is not cryptographic. (Reference [4].)

encipherment: (See *encryption*.)

encryption: The cryptographic transformation of data (see *cryptography*) to produce ciphertext. (Reference [1].)

encryption algorithm: A set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key. (Reference [3].)

end-to-end encipherment: Encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system. (Reference [1].)

end-to-end security: The safeguarding of information in an information system from its point of origin to its intended destination. (Reference [3].)

ephemeral key: A cryptographic key that is generated for each execution of a key establishment process and that meets other requirements of the key type (e.g., unique to each message or session). (Reference [5].)

firewall: A system designed to prevent unauthorized access to or from a private network. (Reference [3].) Firewalls can be implemented in both hardware and software, or a combination of both.

flooding: An attack that attempts to cause a failure in a system by providing more input than the system can process properly. (Reference [4].)

forensics: The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. (Reference [3].)

formal method: Software engineering method used to specify, develop, and verify the software through application of a rigorous mathematically based notation and language. (Reference [3].)

formal security policy: Mathematically-precise statement of a security policy. (Reference [4].)

frequency hopping: The repeated switching of frequencies during radio transmission according to a specified algorithm to minimize unauthorized interception or jamming of telecommunications. (Reference [3].)

gateway: Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures. (Reference [4].)

hacker: Unauthorized user who attempts to or gains access to an information system. (Reference [3].)

hash function: A function that maps a bit string of arbitrary 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 which maps to any pre-specified output; and 2) (Collision-resistant) it is computationally infeasible to find any two distinct inputs that map to the same output. (Reference [5].)

hash-based message authentication code, HMAC: A message authentication code that uses a cryptographic key in conjunction with a hash function. (Reference [3].)

identification: The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. (Reference [3].)

identity: The set of physical and behavioral characteristics by which an individual is uniquely recognizable. (Reference [3].)

identity-based access control: Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity. (Reference [4].)

identity-based security policy: A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed. (Reference [1].)

information assurance: 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. (Reference [3].)

information security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (Reference [4].)

information security architecture: An embedded, integral part of the enterprise architecture that describes 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. (Reference [4].)

information security policy: Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information. (Reference [4].)

information systems security engineer: Individual assigned responsibility for conducting information system security engineering activities. (Reference [3].)

information systems security engineering: Process that captures and refines information security requirements and ensures their integration into information technology component products and information systems through purposeful security design or configuration. (Reference [3].)

initialization vector: A vector used in defining the starting point of a cryptographic process. (Reference [5].)

integrity: (See *data integrity*.)

Interconnection Security Agreement, ISA: Written management authorization to interconnect information systems based upon acceptance of risk and implementation of established controls. (Reference [3].)

Internet Protocol Security, IPsec: Suite of protocols for securing Internet Protocol (IP) communications at the network layer, layer 3 of the OSI model by authenticating and/or encrypting each IP packet in a data stream. (Reference [4].)

NOTE – IPsec also includes protocols for cryptographic key establishment. (Reference [4].)

intranet: A private network that is employed within the confines of a given enterprise (e.g., internal to a business or agency). (Reference [2].)

intrusion detection system, IDS: Hardware or software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from with the organizations). (Reference [3].)

intrusion prevention system: System(s) which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. (Reference [4].)

jamming: An attack in which a device is used to emit electromagnetic energy on a wireless network's frequency to make it unusable. (Reference [4].)

key: (See *cryptographic key*.)

key confirmation: A procedure to provide assurance to one party that another party actually possesses the same keying material and/or shared secret. (Reference [5].)

key derivation: A function in the lifecycle of keying material; the process by which one or more keys are derived from a shared secret and other information.. (Reference [5].)

key distribution: The transport of a key and other keying material from an entity that either owns the key or generates the key to another entity that is intended to use the key. (Reference [5].)

Key-Encryption-Key, KEK: Key that encrypts or decrypts other keys for transmission or storage. (Reference [3].)

key establishment: A function in the lifecycle of keying material; the process by which cryptographic keys are securely established among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement). (Reference [5].)

key exchange: The process of exchanging public keys (and other information) in order to establish secure communications. (Reference [3].)

key length: The length of a key in bits; used interchangeably with 'Key size'. (Reference [5].)

key management: The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction. (Reference [5].)

key management policy: The key management policy is a high-level statement of organizational key management policies that identifies high-level structure, responsibilities, governing standards and recommendations, organizational dependencies and other relationships, and security policies. (Reference [5].)

key pair: Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and 2) even knowing one key, it is computationally infeasible to discover the other key. (Reference [4].)

key recovery: A function in the lifecycle of keying material; mechanisms and processes that allow authorized entities to retrieve or reconstruct keying material from key backup or archive. (Reference [5].)

key revocation: A function in the lifecycle of keying material; a process whereby a notice is made available to affected entities that keying material should be removed from operational use prior to the end of the established cryptoperiod of that keying material. (Reference [5].)

key stream: Sequence of symbols (or their electrical or mechanical equivalents) produced in a machine or auto-manual cryptosystem to combine with plain text to produce cipher text, control transmission security processes, or produce key. (Reference [3].)

key transport: A key establishment procedure whereby one party (the sender) selects and encrypts the keying material and then distributes the material to another party (the receiver). (Reference [5].)

key update: A function performed on a cryptographic key in order to compute a new, but related, key. (Reference [3].)

key wrapping: A method of encrypting keys (along with associated integrity information) that provides both confidentiality and integrity protection using a symmetric key. (Reference [5].)

keying material: The data (e.g., keys and IVs) necessary to establish and maintain cryptographic keying relationships. (Reference [5].)

least privilege: The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. (Reference [4].)

link-by-link encipherment, link encryption: The individual application of encipherment to data on each link of a communications system. (Reference [1].)

malicious software, malware: Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an IS. (Reference [3].)

man-in-the-middle-attack, MitM: A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association. (Reference [4].)

masquerading: The pretense by an entity to be a different entity. (Reference [3].)

master key: A symmetric master key is used to derive other symmetric keys (e.g., data encryption keys, key wrapping keys, or authentication keys) using symmetric cryptographic methods. (Reference [5].)

meaconing: A system of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations. (Reference [7].)

memorandum of understanding/agreement, MOU/A: A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. With respect to security, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. (Reference [3].)

message authentication code, MAC: A cryptographic checksum that results from passing data through a message authentication algorithm. (Reference [3].)

message digest: A cryptographic checksum typically generated for a file that can be used to detect changes to the file. Synonymous with hash value/result. (Reference [3].)

multi-factor authentication: (Also known as ‘strong authentication’.) Authentication using two or more factors to achieve authentication. Factors include: 1) something you know (e.g., password/Personal Identification Number [PIN]); 2) something you have (e.g., cryptographic identification device, token); or 3) something you are (e.g., biometric). (Reference [6].)

mutual authentication: The process of both entities involved in a transaction verifying each other. (Reference [4].)

mutual suspicion: Condition in which two information systems need to rely upon each other to perform a service, yet neither trusts the other to properly protect shared data. (Reference [4].)

nonce: (Also known as ‘number used once’.) A random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing the transmittal of live data rather than replayed data, thus detecting and protecting against replay attacks. (Reference [3].)

non-repudiation: (See also *repudiation*.) Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. (Reference [3].)

one-time password: A password used only once and then permanently discarded.

over-the-air key distribution, OTAD: Providing electronic key via over-the-air rekeying, over-the-air key transfer, or cooperative key generation. (Reference [4].)

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. (Reference [4].)

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. (Reference [4].)

padding: Fill data required by certain cipher modes.

passive threat: The threat of unauthorized disclosure of information without changing the state of the system. (Reference [1].)

password: A string of characters (letters, numbers and other symbols) that are used to authenticate an identity, to verify access authorization or to derive cryptographic keys. (Reference [5].)

peer-entity authentication: The corroboration that a peer entity in an association is the one claimed. (Reference [1].)

phishing: A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information. (Reference [4].)

plaintext: Unencrypted information. (Reference [3].)

private key: In an asymmetric cryptography scheme, the private or secret key of a key pair which must be kept confidential and is used to decrypt messages encrypted with the public key or to digitally sign messages, which can then be validated with the public key. (Reference [3].)

private network: (See *intranet*.)

privilege: A right granted to an individual, a program, or a process. (Reference [4].)

privilege management: The definition and management of policies and processes that define the ways in which the user is provided access rights to enterprise systems. It governs the management of the data that constitutes the user's privileges and other attributes, including the storage, organization and access to information in directories. (Reference [4].)

public key: A cryptographic key that may be widely published and is used to enable the operation of an asymmetric cryptography scheme. This key is mathematically linked with a corresponding private key. Typically, a public key can be used to encrypt, but not decrypt, or to validate a signature, but not to sign. (Reference [3].)

public key cryptographic algorithm: A cryptographic algorithm that uses two related keys: a public key and a private key. (Reference [5].)

NOTE – The two keys have the property that determining the private key from the public key is computationally infeasible. (Reference [5].)

public key infrastructure, PKI: Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. (Reference [3].)

random number generator, RNG: A process used to generate an unpredictable series of numbers. Each individual value is called random if each of the values in the total population of values has an equal probability of being selected. (Reference [3].)

rekey: To change the value of a cryptographic key that is being used in a cryptographic system/application. (Reference [4].)

replay attacks: An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access. (Reference [3].)

repudiation: Denial by one of the entities involved in a communication of having participated in all or part of the communication. (Reference [1].)

residual risk: The risk remaining after risk treatment. (Reference [2].)

risk: Possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability. (Reference [3].)

risk analysis: Systematic use of information to identify sources and to estimate the risk. (Reference [2].)

risk management: The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. (Reference [4].)

NOTE – Risk management includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations. (Reference [4].)

risk mitigation: Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. (Reference [4].)

risk treatment: Process of selection and implementation of measures to modify risk. (Reference [4].)

rule-based security policy: A security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users. (Reference [1].)

secret key: A cryptographic key that is used with a symmetric cryptographic algorithm that is uniquely associated with one or more entities and is not made public. The use of the term 'secret' in this context does not imply a classification level, but rather implies the need to protect the key from disclosure. (Reference [3].)

secret key algorithm: (See *symmetric encryption algorithm*.)

secret (symmetric) key infrastructure, SKI: Cryptographic key infrastructure used to generate and distribute secret (symmetric) keying material such as master keys, key encryption keys, and traffic protection keys.

secure hash algorithm, SHA: A hash algorithm with the property that 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. (Reference [3].)

security association, SA: A relationship established between two or more entities to enable them to protect data they exchange. (Reference [4].)

security policy: The set of criteria for the provision of security services (see also *identity-based security policy* and *rule-based security policy*). (Reference [1].)

security controls: 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. (Reference [3].)

security mechanism: A device designed to provide one or more security services usually rated in terms of strength of service and assurance of the design. (Reference [4].)

security parameters index, SPI: An arbitrary 32-bit value that is used by a receiver to identify the security association to which an incoming packet is bound. (Reference [10].)

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. (Reference [4].)

security plan: Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. (Reference [4].)

security policy: A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data. (Reference [4].)

security protocol: An abstract or concrete protocol that performs security-related functions. (Reference [3].)

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. (Reference [4].)

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. (Reference [3].)

session key: (See *ephemeral key*.)

shared secret: A secret value that has been computed using a key agreement scheme and is used as input to a key derivation function. (Reference [5].)

secure hash standard: Specification for a secure hash algorithm that can generate a condensed message representation called a message digest. (Reference [3].)

signed data: Data on which a digital signature is generated. (Reference [4].)

software assurance: The planned and systematic set of activities that ensure that software life cycle processes and products conform to requirements, standards, and procedures. (Reference [12].)

spoofing: (See *masquerading*.)

spread spectrum: A telecommunications technique in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information. Frequency hopping, direct sequence spreading, time scrambling, and combinations of these techniques are forms of spread spectrum. (Reference [3].)

static key: A key that is intended for use for a relatively long period of time and is typically intended for use in many instances of a cryptographic key establishment scheme. Contrast with an ephemeral key. (Reference [5].)

stream cipher: an encryption mechanism that uses a keystream to encrypt a plaintext in bitwise or block-wise manner. (Reference [11].)

symmetric encryption algorithm: Encryption algorithms using the same secret key for encryption and decryption. (Reference [4].)

symmetric key: (See *secret key*.)

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. (Reference [4].)

threat: A potential violation of security. (Reference [1].)

threat analysis: The examination of information to identify the elements comprising a threat. (Reference [3].)

threat assessment: Formal description and evaluation of threat to a system. (Reference [3].)

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. (Reference [4].)

traffic encryption key, TEK: Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text. (Reference [3].)

traffic protection key: (See *traffic encryption key*.)

transport layer security, TLS: An authentication and security protocol widely implemented in browsers and Web servers. (Reference [4].)

trap door: A hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. (Reference [3].)

trust anchor: A public key and the name of a certification authority that is used to validate the first certificate in a sequence of certificates. (Reference [5].)

NOTE – The trust anchor's public key is used to verify the signature on a certificate issued by a trust anchor certification authority. The security of the validation process depends upon the authenticity and integrity of the trust anchor. Trust anchors are often distributed as self-signed certificates. (Reference [5].)

Trojan horse: A program containing hidden code allowing the unauthorized collection, falsification, or destruction of information. (Reference [3].)

trust: Confidence that an entity, to which trust is applied, will perform in a way that will not prejudice the security of the system of which that entity is a part. (Reference [8].)

validation: Confirmation, through the provision of objective evidence, that the requirements (2.63) for a specific intended use or application have been fulfilled. (Reference [9].)

verification: Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled. (Reference [9].)

virtual private network, VPN: Protected information system link utilizing tunneling, security controls, and end-point address translation giving the impression of a dedicated line. (Reference [3].)

virus: Self-replicating, malicious code that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence. (Reference [3].)

vulnerability: Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited to violate system security policy and result in a security breach. (Reference [3].)

vulnerability analysis: (See *vulnerability assessment*.)

vulnerability assessment: Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. (Reference [3].)

worm: A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread itself. (Reference [3].)

X.509 certificate: The X.509 public-key certificate or the X.509 attribute certificate, as defined by the ISO/ITU-T X.509 standard. (Reference [5].)

X.509 public key certificate: A digital certificate containing a public key for entity and a name for the entity, together with some other information that is rendered unforgeable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard. (Reference [5].)

zero fill: To fill unused storage locations in an information system with the representation of the character denoting ‘0’. (Reference [4].)

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. (Reference [4].)